

Mihaela Cîrlugea

Economie Digitală și Servicii Electronice



U.T.PRESS

Cluj-Napoca, 2025

ISBN 978-606-737-825-2

Mihaela CÎRLUGEA

Economie Digitală și Servicii Electronice



U.T.PRESS

Cluj - Napoca, 2025

ISBN 978-606-737-825-2



Editura U.T.PRESS
Str. Observatorului nr. 34
400775 Cluj-Napoca
Tel.: 0264-401.999
e-mail: utpress@biblio.utcluj.ro
www.utcluj.ro/editura

Recenzia: Prof.dr.ing. Ovidiu Aurel Pop
Prof.dr.ing. Sorin Adrian Hintea

Pregătire format electronic on-line: Gabriela Groza

Copyright © 2025 Editura U.T.PRESS
Reproducerea integrală sau parțială a textului sau ilustrațiilor din această carte este posibilă numai cu acordul prealabil scris al editurii U.T.PRESS.

ISBN 978-606-737-825-2

PREFAȚĂ

Această lucrare se adresează în primul rând, dar nu numai, studenților de la master, care sunt interesați de materia „Economie digitală și servicii electronice”.

Ca și oricare altă carte, consider că și aceasta este o perspectivă de sinteză a autoarei asupra acestui domeniu, mai ales că această zonă de explorare este foarte vastă și conține multe sub-domenii, după părerea mea, fiind aproape imposibil de parcurs integral și eficient integral, mai ales că, noțiunile vehiculate fac parte, multe dintre ele, din varii domenii actuale, care se modifică și se îmbogățesc pe zi ce trece și se modifică odată cu tehnologia.

Doresc să menționez că s-ar putea ca unele idei, definiții sau paragrafe să fie reluate, fie cu alte cuvinte, fie dezvoltate ulterior. Acest lucru este făcut cu intenție, deoarece mintea fiecărui om rezonază cu anumite forme de exprimare, astfel încât, poate unuia îi este mai clară și mai intuitivă o definiție, altui om, altă definiție. De asemenea, prin repetiție, ideile și noțiunile se fixează mai bine în memoria umană, iată un alt motiv pentru care prefer să reiau de multe ori informațiile. Repetițiile se vor regăsi atât în această carte, dar ele se regăsesc și atunci când predau, elementele importante sunt reluate și reamintite la mai multe cursuri, pentru ca acestea să fie înțelese și memorate, scopul fundamental fiind acela ca informația să fie fixată și aprofundată.

***“Know where you are,
find out where you want to go
and plan how to get there”***
Business mantra

I. Comerțul electronic

Comerțul electronic este o activitate tranzacțională de afaceri în cadrul căreia părțile interacționează electronic, nu prin schimb fizic sau contact direct; poate fi interpretată la modul cel mai simplist ca și un schimb de mărfuri, o relație de vânzare-cumpărare, folosind internetul. Schimbul se realizează între o organizație și un deținător de bunuri, intermediat prin informație electronică, care are ca scop dezvoltarea competitivității unei organizații/companii, oferind informații inovație și tehnologii de comunicare prin linkuri/legături spre parteneri și clienți, ajutând la amplificarea activității de marketing a acestor organizații.

Într-o accepțiune primară, noțiunea de comerț electronic se poate referi la cumpărăturile realizate prin internet, adică la un schimb de produse, care se desfășoară în mediul virtual, nu prin acțiune fizică directă. Pe lângă partea efectivă de cumpărare, când vorbim despre comerț electronic, ne putem referi și la:

- **diferite schimburi de servicii sau marfă**
- procese de **negociere între companii**
- precum și acțiuni **de aprovizionare**
- **angajare**
- **planning**
- **transferuri de contracte**
- **transferuri de imagini, fișiere vocale, etc**
- **transmiterea de informații la distanță**

Această activitate de schimburi care are loc prin **mijloace electronice**, se efectuează cu ajutorul calculatoarelor, a asistentului personal digital PDA (personal digital assistant), a telefoanelor

mobile sau prin sisteme de telecomunicații. Comerțul în sine se poate desfășura în principal prin internet, implicând diferite **proces**e:

- **tehnologia internetului**
- **cea al comerțului mobil**
- **transferul de fonduri**
- **administrarea lanțului de aprovizionare**
- **marketing online**
- **procesarea tranzacțiilor online**
- **sisteme de plăți**
- **schimbul electronic de informații**
- **managementul sistemelor de inventariere**
- **un sistem de colecții de date automatizat** .

În general, în aceste situații descrise mai sus, în tranzacție sunt implicați un plătitor și un destinatar, precum și o sumă de bani și-sau informații, schimburile dintre cele două părți având loc în domeniul virtual.

Comerț - Economie	Electronic - Tehnologie
Companii, deținător de bunuri Clienți, parteneri Cumpărături Schimburi de servicii Negocieri între companii Aprovizionare, angajare, planning	Informație electronică Tehnologii de comunicare Internet Mediu virtual Transfer de imagini, fișiere și alte informații la distanță
Marfă fizică	Marfă digitală

- Specific comerțului digital = **Marfa digitală**: template (șablon, tipar, structură), tools (unelte), clase-ore online, produse care se pot descărca (downloadable) cum ar fi lecții, lucrări de artă, fotografii sau tipare printabile, muzică, filme, etc
- Exemple de **servicii** în sfera digitală: freelance writing, content writing, influence marketing, online coaching, arhitectura și designul web

Din punctul de vedere al noțiunilor și activităților implicate, e-commerce poate fi privit:

- Dintr-o perspectivă a **comunicării**, și anume oferta de informații, produse sau servicii, precum și plata prin metode electronice

- Dintr-o perspectivă de **business**, ca și aplicare a tehnologiei pentru automatizarea tranzacțiilor în business și a gestionării fluxului de lucru
- Din perspectiva unor **servicii**, permițând reduceri de costuri pe de-o parte și creșterea vitezei precum și a calității de livrare a produselor
- Din perspectiva **online**, cumpărarea și vânzarea online, precum și obținerea de informații în mediul online

Atunci când guvernul UK a explicat celor din industrie noțiunea și scopul comerțului electronic, acesta l-a definit într-un mod larg:

Comerțul electronic este schimbul de informații prin rețeaua electronică, considerând orice etapă a lanțului de distribuție/aprovizionare, sau, în cadrul unei organizații, schimbul de informații între afaceri, între afacere și consumatori, sau între sectorul public și cel privat, fie ca aceste schimburi sunt plătite sau nu sunt plătite.

Această definiție arată clar faptul că, după cum s-a precizat și mai sus, comerțul electronic, include pe lângă procese de vânzare-cumpărare și activități care au loc înainte sau după cumpărarea propriu-zisă, din lanțul de distribuție. Comerțul electronic este facilitat de mijloacele tehnologiei digitale, care cuprind comunicațiile internet prin site-uri web sau e-mail, dar și mediul wireless sau mobil, precum și medii de furnizare de televiziune, cum ar fi cablul sau satelitul.

Din punctul de vedere al **cumpărătorului**, *avantajele* comerțului electronic pot fi:

- Cumpărătorul poate „vizita” un număr foarte mare de magazine, într-un timp scurt, magazine care pot fi localizate în întreaga lume
- Nu există nicio limită de timp sau spațiu pentru cumpărături
- Cumpărătorul poate vedea ușor diferențele de preț sau calitate între diferitele produse, având astfel o posibilitate mult mai mare de a alege și de a se decide pentru acel produs care să îi satisfacă cel mai bine nevoia; poate foarte ușor și rapid să compare caracteristicile produselor similare aflate pe site-uri diferite
- Cumpărătorul poate primi suport tehnic de la compania vânzătoare și informații în timp real (tip chat) referitoare la produsele de care este interesat
- Posibilitatea clientului de a-și customiza produsul (culoare, material etc)

- Comoditate, deoarece cumpărăturile se pot face de acasă sau chiar în timpul serviciului

Pentru **companiile** implicate în această activitate a comerțului electronic, *avantajele* ar fi următoarele:

- Se poate comunica aproape instantaneu cu alte companii, deci se obține creșterea vitezei de comunicare, indiferent de locația acestora; se păstrează mult mai ușor legătura între companii
- Se pot realiza platforme de cooperare pentru a dezvolta anumite produse, chiar dacă părțile implicate în producție se află localizate în diferite părți ale globului; deci se reduce și minimizează distanța dintre organizații, permițând o colaborare optimă ca timp și posibilitate de acces și comunicare
- Reducerea costurilor (comunicare prin telefon, poștă sau curier, se reduce consumul de hârtie)
- Se pot realiza mult mai ușor studii referitoare la un număr mult mai mare de clienți decât ar fi posibil prin comerțul tradițional
- Este un mod de a dezvolta afaceri între companii
- Posibilitatea comercializării de produse în întreaga lume, dispariția barierelor geografice
- Ușurința de a prezenta noi produse clienților (reclamă/spam), aceștia putând fi puși la curent cu noutățile, update pe produsele existente
- Posibilitatea de a avea costuri mai mici cu un magazin virtual, decât cu magazinul sau magazinele fizice (chirie spațiu, cheltuieli electrică, încălzire, salarii vânzătoare, etc)
- Furnizare de informații despre companii, mai rapid online decât prin telefon, poștă sau alte canale
- Menținerea contactelor cu partenerii, clienții sau furnizorii

Unele **dezavantaje** ale comerțului online ar fi:

- Lipsa interacțiunii umane
- Lipsa experienței simțurilor (atingere, miros, etc) în alegerea produsului
- Situațiile de returnare a produselor și de restituire a banilor
- Costurile de transport care apar și care pot fi uneori mai mari decât costul produsului
- Adaosurile cauzate de vamă și alte taxe, care cresc costul final

- Problemele de securitate, deoarece protocolul TCP/IP care stă la baza comerțului electronic nu are incluse servicii de securitate
- Probleme de urmărire a tranzacțiilor sau, uneori și a produselor
- Pot apare diferențe de limbă și de cultură
- Website care să nu funcționeze din cauza traficului prea mare de internet
- Trimiterea de e-mailuri cu reclame poate cauza neplăcerea, nemulmirea clienților care sunt bombardați cu asemenea mesaje și pierderea acestora; de asemenea acest lucru poate fi împotriva legii
- Mesajele de reclamă pe email ajung în spam sau nu ajung la clienții potriviți și mesajul se pierde
- Produsele comandate se pot pierde și acestea nu mai ajung la cumpărători, situație care aduce prejudicii clientului și/sau vânzătorului, în funcție de clauzele vânzării

Sistemele de plată folosite sunt cardurile bancare, cecuri electronice, ordine de transfer și scrisori de credit electronice și alte posibile metode bancare care pot fi transpuse și procesate în format electronic.

Un aspect important care trebuie avut în vedere este **confidențialitatea** informațiilor care sunt procesate, păstrate și transmise, precum și securitatea tranzacțiilor. Aspecte importante în efectuarea plăților sunt, pe de-o parte realizarea unei interfețe care să funcționeze și să fie operabilă indiferent de dispozitivul de pe care se lucrează sau se face tranzacția, precum și asigurarea unui mediu pentru plăți globale, indiferent de țară, și care să poată prezenta evidențe contabile.

Se disting două categorii mari de activități care definesc comerțul, una definește perspectiva vânzătorului, cealaltă perspectiva cumpărătorului.

Buy-side e-commerce- comerțul electronic din perspectiva vânzării, presupune tranzacții între o organizație care face achiziții și furnizorii acesteia; tranzacții necesare pentru procurarea de resurse luate de la furnizori; tranzacții ale comerțului electronic care au loc între o organizație, furnizorii săi și orice alți parteneri

Conțin în structură, furnizori, furnizorii furnizorilor, și intermediarii. Intermediarii fac legătura, prin internet, cu latura Sell-side.

Sell-side e-commerce- tranzacții dintre o organizație furnizoare și clienți; presupune tranzacții care implică vânzarea de produse clienților unei organizații; tranzacții ale comerțului electronic care au loc între o organizație și clienții acesteia.

Conțin în structură clienți, clienții clienților, care, prin intermediari, fac legătura, prin internet, cu latura buy-side.

Deci, comerțul electronic realizează un schimb între două părți. Pe lângă acesta se poate define Business-ul electronic (E-Business) care conține atât comerțul electronic cât și totalitatea tranzacțiilor electronice din interiorul unei firme sau organizații. Altfel spus, noțiunea de **E-Business** poate fi privită ca și transformarea proceselor cheie de business pentru ca acestea să utilizeze tehnologiile internetului, tehnologiile online. E-business-ul se găsește definit din două perspective.

Primul concept poate fi aplicat activităților de strategie și operațiuni, de exemplu: "organizația noastră are nevoie de o strategie de business mai bună". Prima este bazată pe business-ul bazat pe tipurile de bunuri vândute, proces care implică comanda produsului din mediul digital sau produse tradiționale și servicii, până la alte servicii care facilitează alte tipuri de comerț electronic. A doua categorie este bazată pe natura participanților, astfel putând exista:

B2B, B2C, C2B și C2C (BB=Business, C=Client). Detaliem în continuare aceste tipuri de colaborări între firme și consumatori.

B2B = tranzacții comerciale între o organizație și alte organizații (marketing interorganizațional)

La acest tip de comerț se folosesc intens tehnologiile online, apărând relații comerciale între companii și alte organizații. Avantajul în mediul online, este că, în prezent relaționarea este mult mai ieftină decât era înainte de existența internetului. Alte avantaje se referă la scăderea costului mărfii, eficiența în logistică, scăderea costurilor de vânzare.

Exemple: Eurooffice (tranzacțional), BP (crearea de relații), publicația business Emap (media)

B2C = tranzacții comerciale între o organizație și consumatori persoane fizice. Vânzătorul prezintă produsele sau serviciile online într-un catalog electronic, de unde cumpărătorul are posibilitatea să aleagă, eventual să citească recomandări și să afle metodele de

plată. Plata poate fi fie prin instrumente electronice, fie prin plata ramburs la livrare.

Exemple: Amazon (tranzacțional), BP (crearea de relații), Unilever (creare de brand), News Corp (proprietar de brand media), Kelkoo, Pricerunner (comparatoare de prețuri)

C2C = tranzacții financiare sau informaționale private între consumatori, de obicei mediate printr-un site de business

Exemple: eBay, Skype, MySpace, Bebo, Betfair (serviciu de gambling)

C2B = clienții persoane fizice abordează un business printr-o ofertă

În **al doilea** concept, noțiunea de e-business se folosește ca un atribut pentru a descrie comerțul care se execută în mediul online, adică nu are prezență fizică și urmărește minimizarea serviciilor pentru clienți prin 'web self-service'. Acestea din urmă sunt găsite sub denumirea de 'pureplays'. Ca și afaceri online, în prezent se consideră că cele mai mari organizații din acest al doilea tip sunt Amazon și eBay.

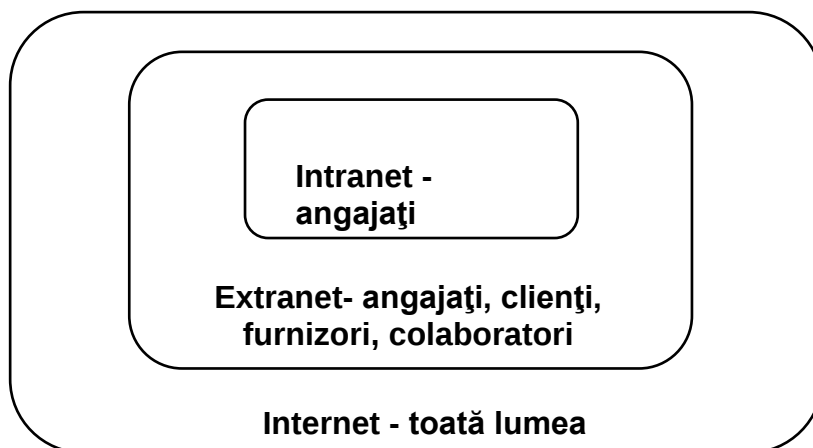
Din punct de vedere tehnic, crearea oricărui sistem de e-business se bazează pe aplicații soft, structuri hardware tip computer precum și structura de rețele, care toate împreună permit unei organizații să desfășoare activitatea de comerț electronic. Important pentru aceste organizații este faptul că trebuie ca modelul de business să aibă integrate partea informațională și tehnologia de comunicații în procesele sale interne, de business. Deci este practic o structură economică modelată, re-modelată sau reinventată pentru a se mula pe structurile și cerințele electronice și virtuale. Ca atare, comerțul electronic poate fi privit ca un sub-domeniu al e-business-ului, deoarece nu se ocupă efectiv de procese specifice unui business, cum ar fi de exemplu prelucrarea comenzii și trimiterea ei.

Tipuri de aplicații care au legătură cu comerțul electronic:

- Comerțul la nivel conversațional, via chat
- Grupuri interesate de știri
- Teleconferințe
- Mesagerie instant
- Portofelul electronic
- Automatizarea documentelor în logistică
- Cumpărarea de bilete electronice

- Enterprise Content Management
- Banking online
- Cumpărare online și urmărirea(tracking) produsului
- Printare la cerere
- Softul tip „Shopping Cart”
- Rețelele de socializare
- Asistentul virtual (componentă de inteligență artificială)
- Sistemul de plăți domestic internațional

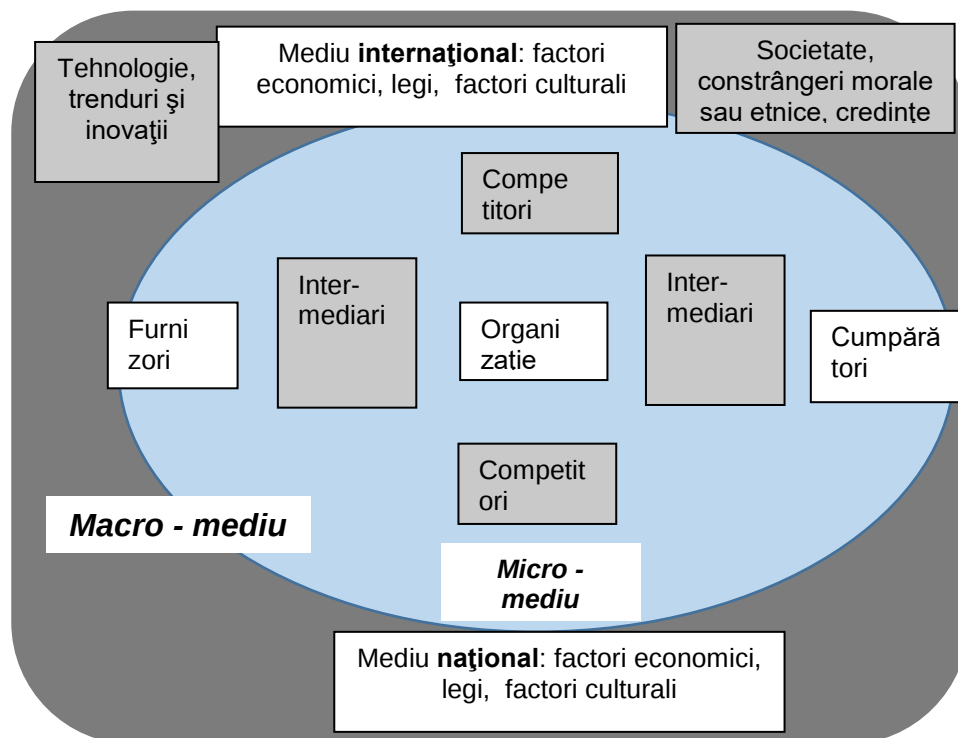
În ceea ce privește spațiul electronic și virtual, distingem noțiunea de Internet, ca și spațiu la care orice business sau client are acces, fiind deci un spațiu universal, accesibil de oriunde de către oricine. Dar, există informații care sunt limitate doar pentru angajații unei firme sau pentru șefi și parteneri. Acestea nu trebuie să fie publice, ca atare ele sunt accesibile doar din interiorul unei organizații. Rețeaua internă a unei organizații care folosește standarde de internet dar doar angajații accesează anumite informații, este numită **intranet**. Poate apare totodată și noțiunea de **extranet**, ca și serviciul furnizat prin internet, la care au acces atât angajații din intranet cât și clienții, furnizorii sau colaboratorii.



Beneficiile intranetului în cadrul unei firme ar fi, toate cu o creștere de 92-97%, conform studiilor făcute în firme:

- îmbunătățirea schimbului și partajării de informații
- dezvoltarea comunicării
- consistență mărită a informațiilor
- o mai bună acuratețe a informației

Astfel, conform observațiilor și explicațiilor de mai sus, avem în continuare schițat mediul în care se realizează serviciile unui e-business.



În funcție de axarea lor spre cumpărător sau vânzător, siteurile pot fi categorisite conform următoarelor denumiri:

Seller-controlled (controlate de către vânzător) = sunt siteul principal al companiei producătoare și sunt capabile de comerț electronic (exemplu www.dell.com)

Seller-oriented (orientate spre vânzător) = siteuri controlate de o a treia parte, dar reprezentând vânzătorul, cum ar fi agenți de distribuție, de exemplu www.opodo.com o agenție de voiaj pan-europeană care furnizează servicii de zbor și care include mai multe companii de zbor, cum ar fi British Airways, Air France, Alitalia, Iberia, KLM, Lufthansa, Austrian Airlines și Finnair.

Neutre = intermediari care nu sunt controlați de către altcineva, de exemplu www.ec21.com, considerată una din cele mai mari piețe

online B2B, conectând milioane de furnizori și cumpărători din întreaga lume; www.computer.com motoare de căutare orientate pe produse specifice; siteuri comparative cum ar fi www.supermarket.com; spații de licitație www.eBay.com.

Buyer-oriented (orientate spre cumpărător) = intermediari controlați de către cumpărători, de exemplu www.covisint.com, nu folosesc o singură piață de desfacere ci fiecare manufacturier își accesează direct furnizorii prin mediul electronic

Buyer-controlled (controlate de către cumpărător) = www.gxs.com, rețea orientată spre tranzacționări masive de capital și acțiuni.

Perspectiva Sell-Side

Comerțul electronic din perspectiva vânzării, include nu doar vânzarea propriu-zisă de produse dar și folosirea serviciilor de internet pentru servicii de marketing. Este de avut în vedere faptul că nu orice produs permite vânzarea online, sau nu toate se pot vinde în același mod, fapt pentru care strategiile de marketing vor varia, în funcție de tipurile acestor produse. Astfel, este nevoie de diferite strategii și se vizează piețe diferite.

Site-urile **tranzacționale** permit cumpărarea online de produse, vânzarea fiind activitatea principală; aceste site-uri furnizează clienților informații despre produsele aflate în vânzare. Din această categorie fac parte magazinele de vânzare produse, magazinele tip agenție de voiaj, sau servicii bancare online.

Site-uri orientate pe **dezvoltarea de relații**, se referă la furnizarea de informații despre produse, atunci când acestea nu sunt disponibile online; se trimit newsletter pentru noutăți și încurajarea vânzărilor offline.

Site-uri care susțin **dezvoltarea unui brand** sunt acelea în care produsele nu sunt disponibile online, principalul obiectiv fiind susținerea brandului prin dezvoltarea unei experiențe în mediul online; de obicei este vorba despre produse tip en-gros, care se cumpără la preț mic, în volum mare.

Site-uri tip **portal sau de publicații** care furnizează informații, știri sau divertisment. La aceste site-uri, câștigul se obține prin reclame, vânzări bazate pe comision, sau liste de date despre clienți.

Rețelele sociale se pot considera ca făcând parte din această categorie.

Pe lângă **beneficiile tangibile**, vizibile, ale comerțului electronic, cum ar fi:

- creșterea încasărilor datorată creșterii numărului de clienți în mediul online, a creșterii pieței online, a cumpărării repetate
- reducerea costurilor de marketing prin vânzări online, print redus și costuri de distribuție reduse
- reducerea costurilor lanțului de aprovizionare, prin nivel simplificat de inventariere, creșterea competiției între furnizori, timp mai scurt în ciclul de comandă
- reduceri de cost în activități administrative datorate unor rutine de business simplificate, în domeniul recrutării de personal, emiterii și plății facturilor

O organizație are și **beneficii intangibile**, care nu sunt fizice dar au efect benefic asupra firmelor:

- imagine îmbunătățită a firmei prin posibilitatea comunicării online
- dezvoltarea brandului
- comunicare de marketing mai rapidă, inclusiv problemele de PR (Public Relations)
- un mai scurt ciclu de dezvoltare al produsului permițând un răspuns mai rapid la nevoile pieței
- serviciu clienți îmbunătățit
- împlinirea așteptărilor clientului prin prezența unui website
- identificarea de noi parteneri de business și întărirea relațiilor cu partenerii existenți
- un mai bun management al informațiilor de marketing și al informațiilor legate de clienți
- feedback din partea clienților referitor la servicii și la produse

În cazul companiilor mari, se consideră că, comerțul electronic este doar o cale de dezvoltare, de sporire a reclamei companiei și a câștigurilor obținute, ceea ce înseamnă că acestea presupun coexistența clară a celor două, adică atât comerțul prin magazine sau lanțuri de magazine fizice, cât și desfășurarea comerțului electronic pe internet. Eventual acestea două se pot urmări a se face în mod complementar, oferindu-se produse diferite în mediul online față de cel fizic, având promoții în mod alternativ online sau fizic, atrăgând cumpărătorul și dinamizându-l pentru a urmări vânzarea în ambele medii. Acest mod de lucru este mult mai eficace în vânzări,

decât varianta simultană. Dacă produsele și promoțiile sunt simultane și identice, clientul se poate orienta doar spre o cale de cumpărare pe care el o consideră mai comodă, pe când dacă acestea sunt complementare, măcar din curiozitate are tendința de a verifica periodic evenimentele din magazinele preferate. De asemenea pentru companii această variantă este mai benefică, permițând de exemplu rotația produselor nevândute înainte de eliminarea lor sau de transferarea acestora spre outlet-uri.

Astfel dacă vânzarile în mediul online pot oferi prețuri mai mici și o ofertă mai mare de produse, acestea totuși nu pot înlocui experiența fizică a mirosului sau tactilității de exemplu, de asemenea de multe ori este greu să se judece calitatea produsului în mediul online, lucru care este mai evident în mediul fizic.

În ce privește securitatea datelor și a tranzacțiilor financiare, ele trebuie protejate în mediul online. Activitățile de phishing, hacking, cyber vandalism sau spyware sunt reduse sau eliminate prin instrumente cum ar fi firewall, softul de criptare, certificate digitale sau parole. Asupra problemelor de securitate se va reveni într-un capitol ulterior.

Ca o concluzie la cele prezentate mai sus, ar fi faptul că, organizațiile nu folosesc tehnologia pentru a automatiza procesele fizice deja existente, ci urmăresc transformarea și dezvoltarea proceselor de activitate prin tehnologie și internet. Cunoștințele necesare pentru o astfel de activitate sunt din diferite domenii, cum ar fi marketing, vânzări, dezvoltare de produs, manufacturare, logistică, dar și dezvoltarea părții de site pentru reclamă (design grafic, soft), de realizare a cumpărăturii efective (plată și securizare electronică).

În ce privește gestionarea lanțului de aprovizionare, Supply Chain Management, SCM, aceasta reprezintă relația și coordonarea tuturor activităților de la furnizori, parteneri până la clienți. Această activitate conține optimizarea tuturor activităților existente, astfel încât să se obțină eficiența și viteza maximă. Acest lucru este important, deoarece clienții apreciază livrarea rapidă de bunuri și servicii.

Din perspectiva companiei, SCM implică administrarea optimă a activităților de planificare, achiziționare, producție, transport, depozitare, distribuire și serviciul clienți. În acest demers intră și supravegherea cheltuielilor sau creșterea de vânzări, pentru a maximiza profitul unei companii și valoarea acesteia.

În cazul nostru, prin comerț electronic, ne vom referi la toate tipurile de tranzacții electronice dintre organizații și acționari (stakeholder). Un acționar, ca parte interesată a organizației, este o persoană, un grup sau o organizație care este afectată de acțiunile, obiectivele și politicile unei organizații. Acesta poate fi: creditor, director, angajat, guvernul și agențiile acestuia, proprietar, furnizor, o uniune, grupare sau o comunitate din care business-ul companiei își preia resursele. Acționarii pot fi activi, având un rol în dezvoltarea și evoluția proiectului, cum ar fi manager sau angajat, sau pasivi, adică sunt afectați de mișcările din proiect, dar nu le cauzează, cum ar fi sponsorii, furnizorii sau subcontractorii.

Pe lângă modelele clasice de business, internetul a dus la dezvoltarea unor concepte inovative. Noile tehnologii, noile modele de business și abordări în comunicații, duc zi de zi la noi idei și perspective.

Un exemplu de inovare este **Google**, care, începând din 1998 se dezvoltă permanent și preia toate elementele originale și de ultimă oră pe care le consideră de viitor: de la miliarde de pagini web pe care le are în prezent indexate, cu servicii de web mail, reclame de tip pay-per-click, rețele analitice și de socializare. Google a cheltuit cel puțin 23 de miliarde de dolari cumpărând circa 256 de companii (spune Factset).

YouTube	2005	1.65 miliarde \$
AdMob –mobile advertising	2006	750 milioane \$
DoubleClick – online advertising	2007	3.1 miliarde \$
Waze - software de navigare GPS	2007	1.3 miliarde \$
FitBit – consumer electronics	2007	2.1 miliarde \$
ITA Software – călătorii și software	2011	700 milioane \$
Motorola Mobility – telecomunicații Re-vândut spre Lenovo la 2.9 miliarde \$	2012	12.5 miliarde \$
Nest – home automation	2014	3.2 miliarde \$
HTC - telecomunicații	2017	1.1 miliarde \$
Looker – data analytics	2019	2.6 miliarde \$
Siemplify&Mandinant –		

cibersecurity Raxium – augmented reality Vicarous – robotic software MobiledgeX – computing brand BrightBytes –data analytics BreezoMeter – măsoară calitatea aerului	2022	Sume secrete
- a cumpărat JotSpot care a devenit Google Sites		
- a cumpărat compania Voice over IP care devine Google Voice		
- cumpără compania de hostare de servicii web Next New Networks a devenit YouTube Next Lab și Audience Development Group		
In 2023 Google investește cca 400 milioane\$ în start-up-ul Anthropic , care se ocupă de inteligență artificială, rival cunoscut al ChatGPT.		

În ultimul timp, primele 10 companii care au investit în **AI** sunt: Google, Facebook, Amazon, Microsoft, IBM, Baidu, Intel, Alibaba, Tencent, SAP.

Google conduce prin suma investită, cca 30.7 miliarde\$ pentru a-și îmbunătăți search engine si asistentul, Facebook 22.1 miliarde\$ pentru îmbunătățirea experienței utilizatorilor, Amazon a investit 10 miliarde\$ pentru servicii de delivery și de asistență vocală.

Companie	Investiție miliarde dolari	Pentru îmbunătățirea:
Google	30.7	Search engine si asistent
Facebook	22.1	Experiența utilizatorilor
Amazon	10	Servicii de delivery și asistență
Microsoft	10	Produse și servicii ca voice recognition-recunoaștere vocală, natural language processing
IBM	200 mil	Data analytics, asistentul Watson
Baidu	200 mil	Search engine și servicii de mapare
Intel	2	Eficiența energetică și securitatea dispozitivelor electronice
Alibaba	17	Platforma de e-commerce si asistentul

		AliMe
Tencent	70	Mesagerie și servicii online de jocuri
SAP	2	Data analytics și asistentul Leonardo

Iată alte exemple de instrumente noi care au fost dezvoltate grație amplificării fenomenului internet precum și un scurt istoric:

1971-1972	Arpanet, rețeaua pentru transfer de pachete de informații, prima care a implementat protocolul TCP/IP, este folosită pentru o vânzare de cannabis între studenți, între Laboratorul Stanford de Inteligență Artificială și MIT= prima tranzacție în rețea
1979	Michael Aldrich, inventator și antreprenor englez, inventează noțiunea și activitatea de shopping online , sau teleshopping, care face posibile tranzacțiile online dintre consumatori și business-uri, sau între un business și alt business; această activitate inventată teoretic, a devenit viabilă doar după inventarea internetului
1981	Primul sistem de online shopping B2B instalat este în UK și se numește Thomson Holidays
1982	Minitel, serviciul online de videotext este introdus în Franța de Telecom (Poșta PTT) și folosit pentru comenzi online
1983	California State Assembly ține prima conferință despre „comerțul electronic” în Volcano, CA; participă firme cum ar fi CPUC, MCI Mail, Prodigy, CompuServe, Volcano Telephone, Pacific Telesis
1984	Firma SIS/Tesco din Gateshead, UK, devine primul sistem de shopping online B2C
1984	CompuServe lansează Mall-ul Electronic în USA și Canada, care devine primul sistem complet de servicii de comerț electronic
1989	Sequoia Data Corp lansează CompuMarket, primul sistem de e-commerce bazat pe internet ; vânzătorii aveau posibilitatea de a posta produse spre vânzare iar cumpărătorii puteau căuta produsele în baza de date și să facă cumpărături folosind cardul de credit
1990	Tim Berners-Lee scrie primul browser web, WorldWideWeb , folosind un calculator marca NeXT

1992	În Cleveland se deschide un site comercial pentru vânzare de cărți online cu plata folosind cardul de credit (www.books.com)
1994	Netscape lansează browserul denumit Mozilla ; Netscape 1.0 folosește o criptare SSL care asigură securitatea tranzacțiilor
1994	Ipswitch Mail Server devine primul software disponibil online pentru vânzare și download imediat
1994	Apare portalul Yahoo , creat la Universitatea Stanford de către studenții Jerry Yang și David Filo, care au creat inițial un website denumit „Jerry and David's Guide to the World Wide Web”, ca un director de alte site-uri organizat într-o ierarhie. Acesta este apoi redenumit în „Yahoo!” ca și acronim de la „Yet Another Hierarhically Organized/Officious Oracle”
1995	Jeff Bezos lansează site-ul Amazon.com și primele posturi de radio online fără reclame, RadioHK și NetRadio
1995	eBay , site-ul de licitații online, este fondat de către programatorul Pierre Omidar, din San Jose.
1995	AltaVista , motor de căutare, cumpărat apoi în 2003 de către Yahoo, care păstrează brand-ul dar folosește propriile motoare de căutare
1996	Apare Hotmail , serviciu de e-mail, cu marketing agresiv care folosea semnătura de e-mail pentru reclamă; cumpărat de Microsoft în 1997, se estimează pentru suma de 400 milioane USD, redenumit MSN Hotmail, devenind apoi Windows Live Hotmail, înlocuit în 2013 de Outlook
1998	Google , motor de căutare, creat de Larry Page și Sergey Brin, studenți la Stanford University, CA; în prezent dețin 14% din acțiuni și controlează alte 56%
1998	Apar timbre poștale electronice, care se pot cumpăra, descărca și printa de pe web
1999	Blogger – platformă de blog care permite bloguri multi-user; cumpărată de Google în 2003
1999	Grupul Alibaba stabilit în China; este o piață de desfacere online, extinsă și foarte profitabilă
1999	Comerțul global atinge vânzări de 150 miliarde USD
2000	Impulsul dot-com (bubble/boost) – moment de vârf

	pentru foarte multe companii bazate pe internet, care apoi au avut căderi mari sau chiar au fost închise
2001	Wikipedia - enciclopedie deschisă, lansată în ianuarie 2001, devenită cel mai populară enciclopedie de acest tip; ajunge în 2007 în primele 10 cele mai populare site-uri
2002	Last.fm - Internet radio și comunitate, cu origine în UK, cumpărată de CBS în 2007 cu 140 milioane lire sterline
2003	Skype - Telefonie internet, VoIP- voice over internet protocol, cumpărată de eBay în 2005
2003	Second Life - Lume virtuală, lansată în 23 iunie 2003 de către firma Linden Lab din San Francisco, ajunge la 1 milion de utilizatori în 2013, la cca 9 milioane în 2017, dar probabil în prezent are undeva între 6.5-7.5 milioane de utilizatori
2004	Facebook - Rețea de socializare; Facebook cumpără 71 de companii, printre care și WhatsApp Facebook nu a reușit să cumpere Snapchat (în 2013) dar a clonat multe trăsături ale acestuia; a inserat de asemenea o clonă de Snapchat în Instagram
2004	Apare DHgate.com , prima platformă B2B din China
2005	YouTube - Distribuție de video; cumpărată de Google în 2006 cu 1.65 miliarde dolari
2007	Site-ul Business.com este cumpărat de R.H.Donnelley cu 345 milioane USD
2010	Instagram - Rețea de socializare de distribuție de fotografii și video; cumpărată de Facebook în 2012 cu 1 miliard de dolari, din care 300 milioane în bani și restul în acțiuni; Astăzi, 2018, valoarea Instagram este estimată la 100miliarde dolari (Bloomberg)
2012	Vânzarile online ating pentru prima dată 1000 miliarde USD, în lume
2013	Alibaba deține 80% din piața comerțului electronic al Chinei
2014	Comerțul online în USA atinge sume de 294miliarde USD, o creștere cu 12% mai mare decât în 2013
2014	În China sunt 600 milioane de utilizatori internet, creând cea mai mare piață de comerț electronic din lume, ca și valoare a vânzărilor estimată la 899 miliarde USD în

	2016
2015	Amazon realizează mai mult de jumătate din creșterea întregului comerț online, vânzând acțiuni de aproape 500 milioane de unități SKU (Stock Keeping Unit = cod de identificare pentru un produs sau serviciu, prezentat de cele mai multe ori sub forma codului de bare)
2015-2020	Estimare a creșterii pieței online cu 56%, față de piața tradițională la care se așteaptă o creștere de doar 2%
2020-prezent	Variază în funcție de țări și de industrii, în ultimii ani, creșterile nu au mai fost așa mari; un oarecum boom a fost în perioada pandemiei

Întrebări :

- Există asemenea site-uri în țara noastră care să fie profitabile?
- Ce înseamnă pentru un site să fie „de succes”?
- Ce considerați că au site-urile de mai sus (din tabel) în comun, ca să fie de succes? -> se pot face studii de caz pentru fiecare companie menționată mai sus = de urmărit de unde au plecat, unde s-a ajuns, prin ce mijloace, ce strategii au folosit?
- Dacă noțiunile de BUSINESS și COMERȚ se suprapun sau presupun totuși aspecte diferite? De cercetat
- Google – ce a mai cumpărat până în 2024 inclusiv? Cifre de afaceri? Cum și ce fel de activități ale Google le-am putea cuantifica prin cifre? De ce cu cifre? Pt că astfel putem compara Google cu alte companii
- Second Life – ce presupune „Viața” virtuală, online, cum ne influențează în viața de zi cu zi?

Zona marketingului digital este inclusă în comerțul electronic, deoarece descrie administrarea și execuția de marketing folosind mediul electronic, cum ar fi internetul, e-mail, televiziunea interactivă sau mediile wireless în combinație cu informațiile digitale despre clienți, ca și date și comportament. Se urmărește recunoașterea importanței strategice a tehnologiilor digitale și dezvoltarea unei abordări planificate pentru a aduna și a transfera clienții înspre zona online prin comunicații electronice dar și prin comunicarea clasică. După ce se stabilește profilul consumatorului, se acționează prin comunicarea vizată a unor date și informații despre produse care se mulează pe nevoile acestora. Rolul

internetului este acela de a susține marketingul prin canale multiple (digitale, mobile, clasice), care trebuie să dezvolte strategii corespunzătoare adaptate acestor tehnologii.

În domeniul business-ului este nevoie de agilitate în strategie, adică de a fi capabil de a răspunde oportunităților din mediu, de a inova pentru a câștiga un avantaj competitiv pe piață, monitorizând modificările pieței în cadrul unei organizații și evaluând în mod eficient eventuale strategii alternative. Apoi este necesară selectarea, revizuirea și implementarea strategiilor potrivite pentru dezvoltarea afacerii.

Pentru creșterea vânzărilor online, se pune accent pe **search engine marketing(SEM)** și **search engine optimisation(SEO)**, deoarece online, clientul are o posibilitate mai mare de a alege tipul de produse precum și de unde poate să cumpere acele produse. Pentru companie este mai importantă căutarea naturală, organică, față de click-ul pe reclame. Căutarea naturală înseamnă că utilizatorul obține rezultatele în baza unor cuvinte cheie pe care el le introduce într-un motor de căutare. Studiile arată că acest tip de căutare este, psihologic, mai de încredere pentru utilizator, decât click-ul pe reclame plătite. Paginile web care apar listate în urma unei căutări naturale sunt considerate mai credibile. Rezultatele sunt de obicei mai relevante. Sigur că pentru companie efortul este mai mare de a ajunge în topul căutărilor decât la reclama plătită, unde poziția de top ar putea fi obținută mai ușor. De asemenea la căutarea naturală nu există siguranța că utilizatorul ajunge la pagina pe care compania o dorește a fi vizitată, lucru care este însă sigur la reclama plătită.

Rețelele de socializare – sunt servicii bazate pe web care permit indivizilor să își creeze un profil public sau semi-public, o listă de utilizatori cu care ei să se conecteze și să facă schimb de informații, să aibă la rândul lor acces la datele celorlalți utilizatori din sistem, să posteze comentarii și să poată evalua informațiile publicate de alții. Acestea ajută mult strategiilor și obținerii de informații pentru marketing.

II. Noțiunea de Web 2.0

Web 2.0 se referă la web într-o formulă în care se pune accent pe conținutul generat de utilizator, folosirea ușoară de către oricine, chiar și de cei care nu sunt experți, participare și interoperabilitate pentru toți utilizatorii(end-users). Acesta a fost creat

în 1999 de către Darcy DiNucci și apoi popularizat în 2004. Conceptul nu se referă la specificații tehnice, ci la schimbarea modului în care paginile web au fost proiectate și folosite. Tranziția a fost progresivă în timp.

Un site web se dorește să permită utilizatorilor să interacționeze și să colaboreze prin dialog, să creeze conținut propriu într-o comunitate virtuală, în contrast cu primele noțiuni despre web, care era folosit pentru citire și informare, deci pentru o vizualizare pasivă de conținut. Astfel, prin web 2.0 s-au dezvoltat și au evoluat noțiuni precum rețele și medii de socializare, bloguri, wiki, cuvinte “tag” pe situri și linkuri, posibilitatea de împărtășire a filmulețelor video, aplicații web “apps”, platforme colaborative, mashups sau widget-uri.

Widget – o aplicație, un buton sau o funcție componentă a interfeței, pe un site sau într-o rețea de socializare, care permite utilizatorului să realizeze o funcție sau să acceseze un serviciu dintr-un alt site. Conținutul poate fi updatat în timp real, deoarece widget-ul interacționează cu serverul de fiecare dată când este accesat.

Mashup – site-uri web, pagini sau widget-uri care combină funcționalitatea sau conținutul a unui site sau a unei surse de date cu o alta, pentru a crea ceva de valoare diferită pentru utilizatorii web.

Caracteristici ale Web 2.0

Utilizatorul contribuie la conținutul unui site prin comentarii sau publicare de articole, având un cont de utilizator sau un profil pe acel site. Userul se bazează mult pe browser, pentru interfața de utilizator, aplicații soft “apps”, sau facilități de stocare de fișiere. Aceasta transformă rețeaua într-o platformă. Apar noțiuni noi, cum ar fi cele de “self-publishing”, “tagging”, butoane “like”, etc. Deoarece userul poate modifica conținut pe site, acesta se numește că are “arhitectură participativă”. Din păcate, această libertate pe net, aduce și probleme cum ar fi cele de spamming, trolling, cyberbullying, etc. Iată unele proprietăți ale Web 2.0 ilustrate prin unele site-uri, și anume:

- Furnizarea de servicii web și hostarea de aplicații interactive (www.flickr.com, <http://maps.google.com>) sau servicii de blog (Blogger.com, www.typepad.com)

- Susținerea participării publicului, majoritatea acțiunilor fiind de participare comunitară de natură altruistă (Bebo, MySpace, Facebook)
- Încurajarea creării de conținut de către utilizatori, cum ar fi blogurile sau www.wikipedia.com
- Servicii de rating și tagging, adică de evaluare, comentare și etichetare, a serviciilor online, fiind astfel de ajutor altor utilizatori prin categorizarea, clasificarea și relevanța conținutului informațiilor găsite online (<http://del.icio.us>)

Iată unele instrumente pentru evaluarea pieții electronice:

www.alexa.com	Unealtă free oferită de Amazon care furnizează clasamentul de trafic pentru diferite siteuri individuale, comparate cu toate siteurile. Funcționează bine pentru siteuri aflate în primele 100.000
www.hitwise.com	Serviciu plătit dar se pot vedea studii free la http://weblogs.hitwise.com ; monitorizează traficul IP și compară audiența
www.netratings.com www.comscore.com	Serviciu plătit, dar conține informații free în secțiunea “press release”; bazat pe utilizatori “acasa” și “la servici”, care au fost de acord să fie monitorizați
www.abce.org.uk	Serviciu gratuit, dând acces bazei de date referitoare la portaluri, nu la siteuri destinație, care au fost de acord ca siteurile proprii să fie monitorizate pentru a strânge date despre traficul de date
www.forrester.com ; are unele comentarii free pe http://blogs.forrester.com	Serviciu plătit, oferă rapoarte despre utilizarea internetului în sectoare cum ar fi serviciile financiare, retail sau informații referitoare la călătorii și agenții de voiaj.
www.gartner.com www.jupiterresearch.com	Servicii de cercetare pe domenii tehnologice

Exemple de site-uri:

Seller-controlled (controlate de către vânzător): sunt siteul principal al companiei producătoare și sunt capabile de comerț electronic (exemplu www.dell.com)

Seller-oriented (orientate spre vânzător): siteuri controlate de o a treia parte, dar reprezentând vânzătorul, cum ar fi agenți de distribuție, de exemplu www.opodo.com o agenție de voiaj pan-europeană care furnizează servicii de zbor și care include mai multe companii de zbor, cum ar fi British Airways, Air France, Alitalia, Iberia, KLM, Lufthansa, Austrian Airlines și Finnair.

Neutre: intermediari care nu sunt controlați de către altcineva, de exemplu www.ec21.com, considerată una din cele mai mari piețe online B2B, conectând milioane de furnizori și cumpărători din întreaga lume; www.computer.com motoare de căutare orientate pe produse specifice; siteuri comparative cum ar fi www.supermarket.com; spații de licitație www.eBay.com.

Buyer-oriented (orientate spre cumpărător): intermediari controlați de către cumpărători, de exemplu www.covisint.com, nu folosesc o singură piață de desfacere ci fiecare manufacturier își accesează direct furnizorii prin mediul electronic

Buyer-controlled (controlate de către cumpărător): www.gxs.com, rețea orientată spre tranzacționări masive de capital și acțiuni.

<http://www.infoworld.com>

<http://www.techopedia.com>

<http://www.econsultancy.com>

<http://www.historyofinformation.com>

www.cio.gov.uk

www.ogc.gov.uk

www.nma.co.uk – New Media Age

www.revolutionmagazine.com

<http://ebusiness.mit.edu>

<http://ide.mit.edu/>

www.mohansawney.com

Kalakota R, Whinston A: Electronic Commerce. A manager's guide, Addison Wesley publishing Company, SUA, 1997

Dan Vasilache: Plăți electronice, Editura Rosetti Educational, 2004

Dave Chaffey: E-Business and E-Commerce Management, Prentice Hall, UK, 2015

<https://www.internetsociety.org>

www.evry.com

www.mohansawney.com

www.techopedia.com
www.econsultancy.com
<http://www.historyofinformation.com>
<https://www.britannica.com/technology/atomic-clock>
 Istorie și studiu de caz Facebook
<https://www.youtube.com/watch?v=qxhj4ahR4Vg>
<https://www.youtube.com/watch?v=Vc2ceRsGATk>
<https://www.youtube.com/watch?v=GQjuEygcS3A>

III. Economia digitală din perspectiva tehnologică

Într-un model de business electronic, este nevoie de activități și servicii din diverse domenii, de specialiști cu pregătire diferită, care, împreună conlucrează pentru a realiza un tot unitar. Dacă privim structura de e-afacere, din perspectiva tehnică sau tehnologică, o putem structura după sarcini sau atribuții. Astfel am putea împărți modelul în cinci etape, cum ar fi prezentarea din tabelul de mai jos.

1. Servicii de Economie digitală	CRM (customer relationship management) relații cu clienții, lanțul de aprovizionare, exploatarea datelor data mining, sisteme de content management
2. Software de sistem	Browser web, server software, software de rețea, sisteme de administrare a bazelor de date
3. Transport și rețea de net	Rețea fizică și standarde de transport (TCP/IP)
4. Depozitare fizică	Depozitare magnetică permanentă a informațiilor pe servere web, stocare de fișiere de backup sau stocare temporară în memorii RAM

5. Conținut și date	Conținut web (web content) pentru intranet, extranet și site-ul propriu-zis, datele clienților, informații legate de tranzacții și de activitatea de click-uri

CRM (customer relationship management) reprezintă gestionarea relației cu clienții, presupunând anumite reguli de strategii și tehnologii pentru atragerea clienților, reținerea și fidelizarea lor.

Dacă ar fi să detaliem, am putea face următoarea clasificare:

Social CRM = aplicații ce folosesc informații despre clienți obținute din social media pentru a extrage date și statistici

Mobile CRM = pentru a răspunde nevoii de mobilitate a agenților de vânzări

CRM Integrat = este acela în care programul CRM devine o platformă pentru integrarea altor aplicații software de vânzări și marketing, cum ar fi trimiterea de newsletter, centrale telefonice sau trimitere SMS-uri.

Tehnologia Internetului

Prin internet ne referim la rețeaua fizică care leagă, interrelaționează milioane de calculatoare între ele, pe întreg globul. Această rețea este alcătuită dintr-o infrastructură de servere și linkuri de comunicare între aceste servere, utilizate pentru a păstra și transporta informații și date între calculatoarele client și serverele web.

Pentru transferul de date, se transmit cereri (request) de informații de la calculatoarele client sau dispozitive mobile, ale căror utilizatori cer accesul spre servere deținătoare de informații și gazde ale unor aplicații business. Serverele răspund la cereri, furnizând serviciile cerute. Astfel, putem spune că internetul este un sistem enorm de sistem client-server.

O **arhitectură client-server** constă din calculatoare *client*, de tip PC, care împarte resurse cum ar fi baze de date, stocate pe un calculator mai puternic, *serverul*.

Computerele client sunt conectate la internet prin intermediul furnizorilor locali de internet (local internet service providers ISP), legați la rândul lor la provideri mai mari, cu conexiuni la infrastructurile majore naționale sau internaționale, aceste infrastructuri fiind administrate de mari organizații comerciale, de exemplu în Anglia ar fi Verizon sau UUNET. La nivel național se facilitează conectarea infrastructurilor mari pe ISP-uri majore globale, pe un singur link mare spre Europa și spre întreaga lume. Aceste legături de mare viteză sunt un fel de magistrale.

Din punct de vedere fizic, la nivel global, există multe cabluri subterane sau submarine care formează legăturile majore între țări.

Unele companii au administrare proprie de servere sau folosesc ISP, dar cea mai comună cale este de a folosi un furnizor de hosting pentru acest serviciu. De exemplu firma Rackspace (www.rackspace.com) se consideră cea mai mare firmă de hosting a Europei, găzduind din 2001 siteuri importante, aplicații internet, servere de e-mail, servicii de stocare și securitate pentru peste 4000 de clienți, unii chiar în SUA.

Iată mai jos un scurt istoric din punct de vedere tehnologic al internetului.

1958	Atunci când Uniunea Sovietică lansează pe orbită primul satelit Sputnik, în SUA președintele Eisenhower creează NASA (National Aeronautics and Space Administration) și ARPA (Advanced Research Projects Agency), care a inventat precursorul internetului. ARPA trebuia să rezolve problema de comunicare a Departamentului de Apărare a SUA, creând rețeaua de calculatoare ARPANET.
1961	Primul raport de cercetare prezentat despre teoria de schimb de pachete între calculatoare
1966	Primul plan pentru ARPANET
1969	Primul nod este la UCLA în 2 septembrie, urmând alte 4 noduri de rețea în decembrie
1973	Primele conexiuni internaționale între universități: University College din Londra și Royal Radar Establishment, Norvegia
1976	Regina Elizabeth II a Marii Britanii trimite un e-mail
1982	Se adoptă primul standard de protocol, TCP/IP, prima definiție a Internetului

1984	Se introduce sistemul referitor la numele de domeniu (DNS Domain Name System)
1985	Symbolics.com devine primul site înregistrat de tip dot-com
1987	Se dezvoltă structura magistrală NFSNet, care devine în 1988 TI
1988	Virusul Worm afectează 6000 de noduri de rețea din 60000
1989	La NSFNet sunt conectate mai multe țări, cum ar fi Argentina, Austria, Belgia, Brazilia, Chile, Grecia, India, Irlanda, Coreea, Spania, Elveția
1990	Se lansează WorldWideWeb de către institutul CERN(European Organization for Nuclear Research) din Elveția
1992	Apare noțiunea de "surfing"- de navigare pe internet
1993	www are o creștere anuală de 341,634% la serviciul de trafic
1994	Primele mall-uri online, bănci virtuale, online pizza și SPAM
1995	Există Netscape și începe, urmează "războiul" browserelor
1997	Numărul de siteuri web depășește 1 milion
1999	Internetul devine accesibil cu ajutorul telefonului mobil; aproximativ 30 milioane de servere host
2002	2 miliarde de pagini web indexate pe mai mult de 20 de milioane de siteuri web; aproximativ 100 de milioane de servere host
2006	Întinderea largă în toată lumea a blogurilor, RSS feeds și podcasts; aproximativ 350 de milioane de hosts

În ce privește noțiunile de web și internet, se cuvine următoarea precizare:

Internet = sistem global de calculatoare interconectate care realizează schimbul de date prin pachete de date folosind protocolul standardizat de internet (TCP/IP). Astfel, internetul este definit de standardele acestui protocol TCP/IP. Este rețeaua fizică care interconectează calculatoare pe întregul glob; conține infrastructura serverelor și legăturilor de comunicație dintre acestea, folosite pentru

păstrarea și transportul informației dintre PC-urile client și serverele web

WWW = world wide web o reprezintă tehnica cea mai simplă de publicare a informației pe internet, informație care se accesează prin browsere web care afișează paginile web conținând elemente de grafică și text HTML sau XML. WWW este definit ca un spațiu al informației, în care termenii de interes sunt denumiți resurse și sunt accesate prin identificatori globali denumiți URI (uniform resource identifiers). Deci web-ul este un spațiu al informației, este ceva abstract, pe când internetul este prezentat ca și partea hard, cea reală.

Consortiul W3C

Este important a se menționa existența consorțiului **W3C** (World Wide Web Consortium), organizație fondată de către Tim Berners-Lee, inventatorul web-ului, comunitate internațională care se ocupă cu dezvoltarea de standarde și protocoale pentru creșterea internetului pe termen lung. Funcționează pe baza unui cod de etică și profesionalitate. Sunt create structuri și module care ajută web-ul să funcționeze.

W3C nu are un singur sediu, ci sunt 4 sedii importante, și anume: MIT (în Cambridge, MA, USA), ERCIM (în Sophia-Antipolis, France), Keio University (lângă Tokyo, Japan), și Beihang University (în Beijing, China). De asemenea această organizație mai este reprezentată în 17 alte regiuni ale lumii (W3C Offices).

Platforma open web a dus la creșterea considerabilă și rapidă a comerțului. Sume uriașe de bani sunt vehiculate anual pe web, proporția fiind în creștere. Astfel încât industria trebuie să evolueze pentru a realiza următoarele:

- Dezvoltarea de instrumente hard de tip mobil, de acces de semnal în bandă largă, de existența unor medii cu dispozitive multiple pentru accesul la activitatea de comerț online și virtual
- Dezvoltarea instrumentelor de plată cum ar fi portofelul electronic, tehnologii blockchain, alte metode mai rapide de plată
- Apariția și dezvoltarea tehnologiei EMV; această tehnologie este un standard global pentru carduri de credit și de debit, bazate pe tehnologia cu chip; numele vine de la tipurile Europay, Mastercard și Visa, structurile originare care au

dezvoltat această tehnologie globală care face posibil ca o monedă să fie acceptată în toată lumea.

- Tehnologia blockchain care se ocupă de distribuirea unor registre publice financiare ce păstrează informațiile neschimbate într-un loc sigur, asigurând clienții că datele și tranzacțiile sunt protejate, criptate și nealterate. În acest sens avem criptomonede cu tehnologie de tip registru distribuit (distributed ledger technology DLT)
- Alte exemple de tipuri de tranzacții sunt stocările de date, tranzacțiile imobiliare, financiare sau gestionarea activelor (asset management).

Pentru a veni în întâmpinarea nevoilor din industrie în zona www, organizația W3C a înființat Web Commerce Interest Group, grupul de interes pentru comerțul pe web. Această organizație include structuri și informații din domeniul băncilor, emitenți de carduri, companii de comerț electronic, operatori de telecomunicații, vânzători de hardware, de softare și browsere web, alți operatori de servicii multiple. Aceștia modulează tipurile de plăți care se pot efectua pe internet pentru a:

- Reduce rata de abandon a coșurilor de cumpărături
- Crește securitatea plăților și a reduce fraudă
- Promova metodele inovative de plată atât în magazine fizice cât și pe aplicații online
- Facilitarea de programe digitale de loializare și distribuția de cupoane
- Posibilitatea de plăți gen Internet of Things sau realitate virtuală
- Relaționarea metodelor inovative de comerț și plăți cu posibilitățile arhitecturale ale internetului
- Standardizări de tip FIDO, EMV sau 3D Secure

Astfel, există grupuri care se ocupă de:

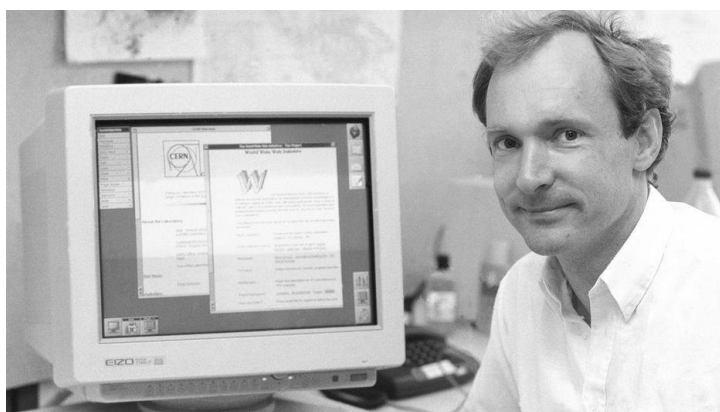
- Plăți online
- Securitate și criptografie web, API care permit dezvoltatorilor să implementeze protocoale sigure la nivelul aplicațiilor web, incluzând confidențialitatea mesajelor și serviciile de autentificare, prin expunerea de funcții criptografiate de încredere primite de la browser
- Certificare(authentication) – pentru securitatea parolelor

- Comunitate pentru securitatea „registrelor” (interledger)- de fapt a rețelelor de plată pe internet
- Ontologia business-ului financiar online
- Active digitale de tip blockchain și comunicare interbancară
- Comunitate digitală
- Senzori și dispozitive care creează API client care permit dezvoltarea de aplicații și widget-uri care să interacționeze cu structuri hardware, cum ar fi senzori, cameră video, microfon și alte aplicații
- Web bluetooth care dezvoltă specificații pentru API de Bluetooth pentru a permite site-urilor web să comunice cu dispozitivele într-un mod securizat și cu păstrarea confidențialității datelor
- NFC –Near Field Communication API

Scurt Istoric

Tim Berners-Lee, om de știință englez, propune în martie 1989 un sistem de administrare a informației care este apoi implementat cu succes în noiembrie 1989, sistem care conduce la ceea ce cunoaștem noi astăzi ca fiind internet-ul, World Wide Web (WWW). Acest sistem implementează prima comunicare de succes HTTP (Hypertext Transfer Protocol) client-server prin intermediul internetului.

Lee a creat o serie de pagini folosind limbajul HTML, legate între ele prin pointere denumite hiperlinkuri (hyperlinks). Ca urmare a acestui lucru a apărut necesitatea unui program care să acceseze și să afișeze corect paginile HTML. Acesta a fost browser-ul. Tim a realizat primul editor de pagini de internet sau browser “WorldWideWeb.app” și a programat primul server web “httpd”. Spre sfârșitul anului 1990, prima pagina web devine disponibilă pe internet.



Până în octombrie 1990, Tim a introdus trei elemente fundamentale care au rămas temelia a ceea ce înseamnă web astăzi: HTML, HTTP și URI.

HTML= HyperText Markup Language, adică limbajul de formatare pentru web;

HTTP = hypertext transfer protocol, deci un protocol de tip text, implicit al www, care permite comunicarea cu site-urile dorite, adică permite accesarea informației dorite de pe internet;

URI = Uniform Resource Identifier. Un fel de „adresă” unică folosită pentru a identifica fiecare resursă de pe internet. În prezent, apare în mod uzual ca și URL.

Dacă ar fi să dezvoltăm noțiunea de HTTP se poate spune că este un protocol de distribuție, de colaborare de sisteme, de informare hypermedia. Este un protocol generic și apatrid folosit pentru a furniza date, cum ar fi fișiere HTML, imagini, rezultate ale unei cereri, etc. Specificațiile acestui protocol declară cum se construiesc interogările și cum sunt trimise la server dar și răspunsul serverelor. Pentru ca acest protocol să fie eficient, sunt necesare trei aspecte a fi îndeplinite:

- Să nu fie necesar un aranjament între părți, pentru ca mesajul să se poată trimite
- Protocolul să nu depindă de media
- Protocolul este apatrid, clienții neavând nevoie să memoreze date pentru a putea comunica

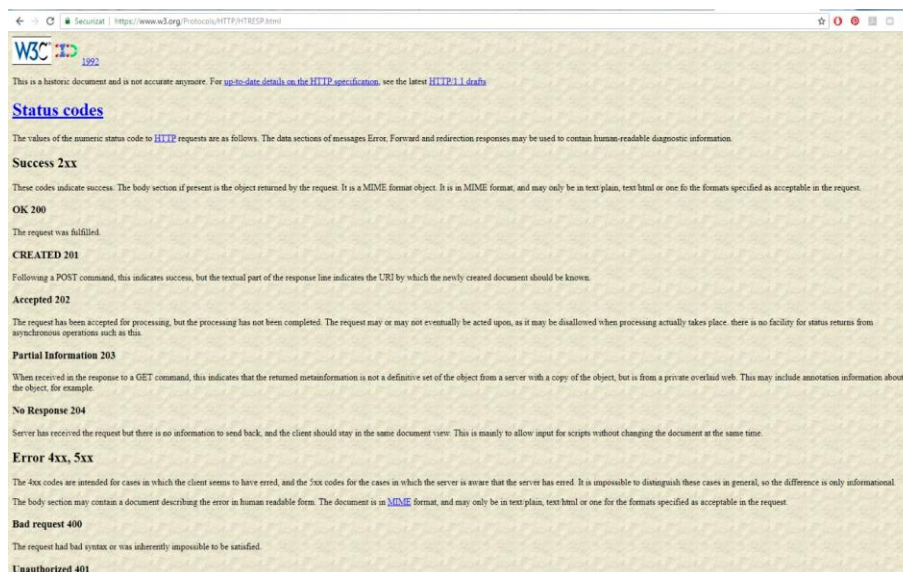
Protocolul se bazează pe o arhitectură client-server, și anume dacă browser-ul și motoarele de căutare devin clienți ai protocolului HTTP cerând diverse resurse, serverul web va răspunde acestor cereri.

Protocolul HTTP este un protocol de cerere/răspuns bazat pe o arhitectură client/server: în cazul în care browser-ul web, roboții și motoarele de căutare acționează precum clienți ai HTTP care cer anumite resurse, serverul web răspunde la cereri.

Prima adresă de pagină de internet a fost

<http://info.cern.ch/hypertext/WWW/TheProject.html>

care prezenta detalii legate de proiectul www. Cei care vizitau pagina puteau afla detalii despre hipertext, detalii tehnice pentru a-și realiza



propria pagină web precum și explicații despre cum să caute informații pe net. Avem mai jos un exemplu de pagină W3C din 1992. Pe măsură ce proiectul lua amploare, structura și datele de pe aceste site-uri erau modificate aproape zilnic de către cei de la Institutul Cern.

Comunitatea W3C se ocupă de stabilirea și dezvoltarea standardelor web. În august 1992 cinci organizații lider mondial au semnat un acord de afirmare și aderare pentru a stabili principiile de dezvoltare a Paradigmei Moderne de Standarde a internetului, un model care va duce la îmbunătățirea radicală a modului în care oamenii din întreaga lume au contribuit inovativ la dezvoltarea de noi tehnologii, benefice pentru umanitate.

Prima comunitate web înființată astfel, a introdus următoarele idei revoluționare referitoare la internet și la disponibilitatea informației:

Descentralizarea: pentru a posta o informație online, nu este nevoie de permisia vreunei autorități centrale. Aceasta implică totodată lipsa cenzurii și a supravegherii centralizate.

Nediscriminarea: toți cei care au acces la internet, independent de suma pe care o plătesc pentru aceste servicii, comunică la același nivel cu ceilalți participanți ai internetului. Acest aspect este cunoscut ca neutralitatea internetului.

Design de tip bottom-up (de jos în sus): codul nu este scris și controlat de către un grup mic de experți, ci el este dezvoltat sub privirile tuturor, încurajând participarea și experimentarea lui de către întreaga colectivitate.

Universalitate: Toți au posibilitatea de a publica orice pe internet, toate calculatoarele care sunt implicate trebuie să comunice între ele prin aceleași limbaje, chiar dacă sursele hardware folosite de utilizatori sunt diferite; de asemenea, la publicarea informațiilor pe internet nu se ține cont de cultură, de credințele religioase sau apartenența politică.

Consens: Pentru ca aceste standarde universale să funcționeze, toată lumea trebuie să fie de acord cu ele. Tim și echipa sa, au obținut acest lucru, dând posibilitatea tuturor să aibă un cuvânt în crearea standardelor, dezvoltând astfel un proces de dezvoltare transparent la W3C.

Cuvinte cheie: Open Data, Open Government, Open Access, Free Culture

Principiile organizației W3C referitoare la internet

Web for All

Se pune accent pe valoarea socială a internetului, care permite comunicarea interumană, comerțul și posibilitatea de a împărtăși cunoștințe. Unul din principalele scopuri ale W3C este ca aceste beneficii enumerate mai sus să fie disponibile întregii omeniri, indiferent de posibilitățile lor hard, soft, a structurii rețelei, indiferent de cultură, limbă, localizare geografică sau abilități mentale sau fizice.

Web for Rich Interaction

Internetul a fost creat ca o unealtă de comunicare care să permită tuturor să distribuie informații. Pentru mult timp, internetul a constituit doar un instrument „read-only” pentru multă lume. Apoi însă au apărut blogurile, „wiki”, rețelele de socializare, acestea făcând posibilă prezentarea de conținut propriu și personalizat, al tuturor participanților la internet. W3C au urmărit să conceapă standarde cu arhitectură puternică și principii robuste de design care să permită aceasta.

Web of Data and Services

Unii utilizatori privesc internetul ca un uriaș depozit (repository) de informații, în timp ce pentru alții, web-ul reprezintă un set de servicii care facilitează schimburile de mesaje între persoane. Aceste două

perspective sunt complementare și se folosesc una sau cealaltă în funcție de necesitate.

Web of Trust

Internetul a modificat modul de comunicare dintre oameni și, ca urmare, natura relațiilor sociale, interumane. Sunt frecvente întâlnirile online atât în relații personale dar și pentru ședințe de servicii sau tranzacții comerciale- afaceri. Uneori persoanele nu ajung niciodată să se întâlnească și în realitate. Pe de-o parte se pot astfel naște relații de încredere dar, pe de altă parte, tehnologia poate priva omul de încredere și confidență.

Web on Everything

În prezent, dispozitivele care pot accesa internetul sunt numeroase, amintim: telefoane mobile smart, PDA(personal digital assistants), sisteme de televiziune interactiva, smartwatch-uri sau alte aparate de uz casnic.

Web of Devices

Dispozitivele electronice sunt prezente în foarte multe variante, au diferite dimensiuni și proprietăți, toate acestea impunând restricții asupra conținutului pe care aceste dispozitive îl pot procesa. Aplicațiile de tip API și CC/PP ajută dezvoltatorii să programeze dispozitivele astfel încât acestea să fie cât mai aproape de dorințele utilizatorului.

Telefoane mobile: W3C promovează un singur internet care este disponibil, spun ei, pe orice dispozitiv de telefonie mobilă, astfel încât să se obțină rezultate bune indiferent de capacitatea dispozitivului, ținând cont și de locație și alte informații care țin de contextul device-ului sau al utilizatorului.

Acces multi-modus: Interacțiunea utilizatorului cu dispozitivele electronice nu mai are loc doar prin intermediul tastaturii, dar și cu ajutorul vocii, a atingerii sau a gesturilor. Arhitectura W3C Multimodală și componentele acesteia (EMMA, InkML), permit adaptarea aplicațiilor la noi moduri de interacțiune.

Navigarea vocală: Cadrul W3C „Speech Interface” este un set de specificații care combină și integrează tehnologia web cu interacțiunea vocală. Astfel de aplicații sunt VoiceXML, PLS, SISR, SRGS, SCXML și CCXML .

Televiziunea: Odată cu apariția dispozitivelor bazate pe ip-uri, transmisia TV tradițională evoluează într-o experiență nouă unde utilizatorul poate interacționa cu aplicații bazate pe tehnologiile web. S-a constatat o creștere a implementării dispozitivelor care

integrează tehnologii web cum ar fi HTML, CSS sau SVG, cuplate cu diferite aplicații de dispozitiv(API).

În 1993 apare un nou browser, denumit Mosaic, care devine utilizat pe scară largă într-un timp foarte scurt, datorită interfeței sale grafice deosebite. Acesta a fost apoi dezvoltat în 1994 de către Marc Andersen, membru al echipei Mosaic, care realizează un browser propriu comercial, și anume Netscape Navigator. Acesta câștigă inițial 90% din piață, dar apoi apare în 1995 Internet Explorer de la Microsoft. Cum Internet Explorer era gratuit, Netscape Navigator a pierdut astfel competiția și a dispărut.

În 2003 este înființată organizația **A4AI** (the Alliance for Affordable Internet). Această organizație include companii ca și Google, Facebook, Intel și Microsoft. Președinte este Sir Tim Berners-Lee. Această organizație urmărește accesibilizarea internetului în toată lumea.

Exemplu de caz- BlendTec

BlendTec – firmă americană care vinde blendere, atât domestice cât și pentru uz profesional, comercial, fondată în 1975 de către Tom Dickinson pe când avea 29 de ani. Înainte de aceasta, a produs moara de bucătărie, care cântărea 3 kg și care producea făină de 2 ori mai repede și mai fină decât moara clasică mare, din piatră, de 30 de kg.

Se spune despre el că a fost un bun inventator și inovator încă de mic, și-a programat soneria de la intrare să deschidă poarta, a dotat karturi cu motoare care au depășit viteza de 80 km/h.

Tom Dickinson a inventat blenderele comerciale cu amestecare de mare viteză, diferite profiluri de amestecare, cicluri preprogramate, interfețe tactile capacitive, lame cu aripioare, 12 aparate într-unul singur, recipiente de măcinare cu 5 fețe, lama cu 80% mai groasă și de 10 ori mai puternică decât aveau celelalte blendere competitive din lume. Tom a inventat primul aparat de smoothie cu autoservire(self-serve smoothie). Astfel, produsele BlendTec au devenit populare și indispensabile în restaurante, baruri, cafenele și case din întreaga lume.

În 2013 câștigă Gold Award for Innovations cu seriile BlendTec Signature și Stealth Lines (serii de blendere). Era important că aceste aparate aveau control asupra vitezei și se puteau programa diferite cicluri de măcinare.

În 2017 primește premiul Kitchen Innovation Award pentru sistemul Nitro Blending, care se mănuieste ușor, controlează bine porțiile, totul se face cu efort minim și în condiții sanitare bune.

În 2021 majoritatea acțiunilor companiei sunt vândute spre grupul Wasatch.

Firma BlendTec are încasări de cca 56mil\$ în 2022, maximul atins, 694 angajați iar venitul per angajat ar fi cca 80 mii \$. Firma este renumită pentru campania virală de marketing **Will it blend?** În fiecare episod Tom Dickinson, fondatorul firmei, sub oarecum motto-ul "Will it blend? That is the question", apoi, după demonstrație, prezentarea se încheie cu : "Yes, it blends!"

S-a construit micro-site-ul www.willitblend.com în care se prezintă un blender, modelul Total Blender, care distruge obiecte precum iPhone, iPod, mingi de golf, cameră video, etc, deși scopul acestui blender era de a produce shake-uri sau smoothies. Au avut o campanie virală atât pe acel site, dar și pe youtube cu propriul canal: www.youtube.com/user/blendtec, având la filmulețe vizionări de 12-18 milioane de vizitatori, iar vânzările fiind crescute cu **500%** datorită acestui canal. Informații pentru ziariști apăreau și pe blogul lor: <http://blog.blendtec.com>. Produsele au fost prezentate însă în reclame și pe canalele clasice, adică la televizor, în ziare, reviste și radio, demonstrând faptul că mediile tradiționale au avut un impact mare în creșterea conștientizării existenței acestor produse, după impactul inițial.

Această campanie este importantă deoarece a început din 2006, într-o perioadă în care încă video-marketing-ul nu era popular. Tom a reușit să demonstreze fiabilitatea produselor sale, puterea și durabilitatea. Acele video-uri au câștigat #1-viral-marketing-campaign-of-all-time honors from AdAge și CLIO international advertising award.

<https://www.w3.org/>

www.salesforce.com

<https://geekhistory.com>

Dave Chaffey: E-Business and E-Commerce Management, Prentice Hall, UK, 2015

www.willitblend.com

<http://blog.blendtec.com>

<https://www.youtube.com/user/Blendtec>

IV. Browsere web

Un browser(navigator) este un soft folosit pentru a afișa și a accesa site-uri pe internet, soft care permite utilizatorului să localizeze, să acceseze și să afișeze pagini web.

Browserele „traduc” paginile web, furnizate ca HTTP într-un conținut inteligibil pentru utilizator. Prin protocolul HTTP, pagina web este accesată și afișată pe ecranul calculatorului. Pe lângă protocoalele HTTP, browserele se mai ocupă și de securitate (HTTPSecure), transfer de fișiere (File Transfer Protocol FTP), trimitere de mesaje/mailuri (mailto) și fișiere propriu-zise (files). De asemenea, majoritatea browserelor suportă module plug-in externe, module care extind funcționalitatea browserului și care sunt necesare pentru afișarea conținutului dinamic, cum ar fi video-uri, secvențe audio sau jocuri.

Este important aici să subliniem diferența între următoarele noțiuni:

HTTP este protocolul implicit al www, protocol de tip text, care trimite cereri către server, fără a utiliza vreun algoritm de criptare a datelor. Ca atare, a se evita o astfel de legătură atunci când avem nevoie să furnizăm date personale sau despre card, cont bancar etc.

HTTPS combină protocolul clasic HTTP cu un alt protocol, dintre acestea **SSL** (Secure Sockets Layer) sau **TLS** (Transport Layer Security) fiind cele mai utilizate. Această variantă este de preferat pentru clienți atunci când transmit informații private pe internet, deoarece, pentru siguranță, datele sunt supuse unui algoritm de criptare și sunt astfel transmise între calculator și server. Criptare înseamnă ascunderea anumitor informații pentru a nu putea fi accesate decât de către cei care au cheia de acces la acestea. Serverul trebuie să aibă un certificat sau o cheie de criptare pentru a descifra informația primită, certificat verificat de o entitate (Certificate Authority) care confirmă că entitatea sau persoana care a emis certificatul este de încredere.

Există browsere cu mai multe tipuri de proprietăți, făcute pentru a rula pe diverse sisteme de operare. Dintre browserele comune amintim Internet Explorer (Microsoft), Firefox (Mozilla), Google Chrome, Safari (Apple) sau Opera. Majoritatea oferă și versiuni lightweight, adică care nu consumă multe resurse, pentru rularea pe telefonul mobil.

Ar fi bine ca fiecare să aleagă și să utilizeze acel browser care îi îndeplinește cel mai bine nevoile, criterii de alegere care pot fi legate de viteză, securitate sau flexibilitate.

Mozilla Firefox



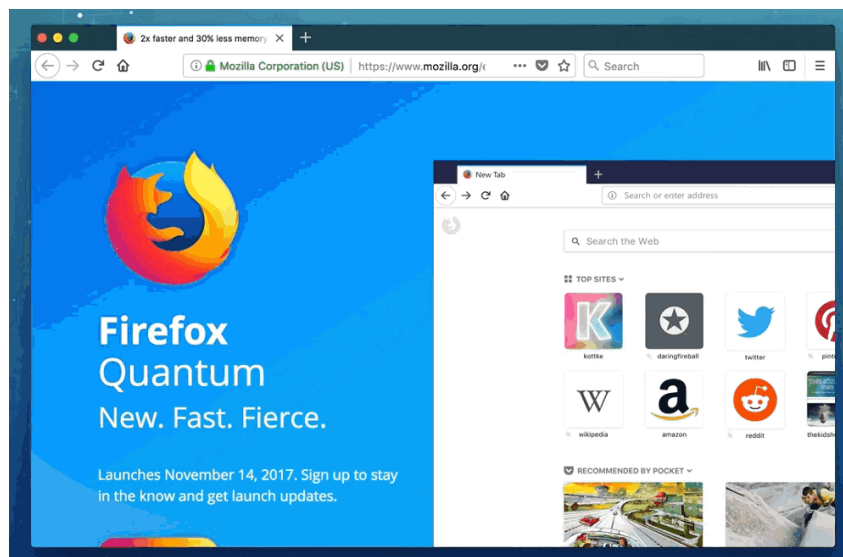
Acest browser dezvoltat de către cei de la Mozilla, rulează sub sisteme de operare cum ar fi: Windows, Mac, Linux, Android, iOS. Acest browser are ca și caracteristici de bază:

- viteza
- interfață cu design foarte eficace
- lucrul ușor cu resursele de sistem
- unelte foarte sigure pentru confidențialitatea și securitatea datelor

Firefox a apărut în 2002 sub numele de „Phoenix”. Era cunoscut și atunci pentru viteză, securitate și add-ons, mai performant decât Microsoft Internet Explorer, care la acea vreme domina piața. Sub numele de Firefox, apare în 2004 și este succesorul „spiritual” al browserului Netscape. În 2009 este folosit de către 32% din utilizatorii de internet. În 2015 apare versiunea pentru iOS. În martie 2018 este folosit doar de un procent de 11.78% din utilizatori, fiind detronat de Google Chrome. El este însă majoritar folosit în Cuba, 78.3% sau Eritrea 91%.

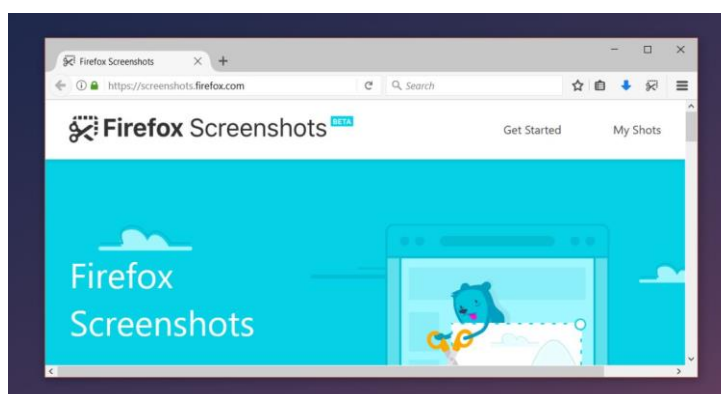
În prezent, Firefox a fost up-datat, astfel încât a ajuns printre cele mai bune browsere. Este foarte flexibil permițând adăugarea de extensii de către useri independenți, dar în ultimii ani, suferea de lipsa de viteză. Firefox Quantum, lansat în 2017, are în prezent viteza comparabilă cu Google Chrome, aceasta chiar și în situații în care memoria RAM este folosită doar puțin, chiar și cu o mulțime de tab-uri deschise. Deși foarte bun la capitolul viteză, totuși Chrome rămâne în fruntea clasamentului în 2018. Browserul este notabil și în ce privește confidențialitatea, Mozilla fiind o fundație non-profit, nu este disperată în a vinde datele personale ale utilizatorilor, cum se

întâmplă în cazul altor browsere! De asemenea efectuează periodic update-uri ale acestor date pentru a proteja informațiile legate de useri. Firefox Quantum a introdus un sistem pentru extensii care previne developerii cu intenții rele de a face modificări în codul intern al browserului.



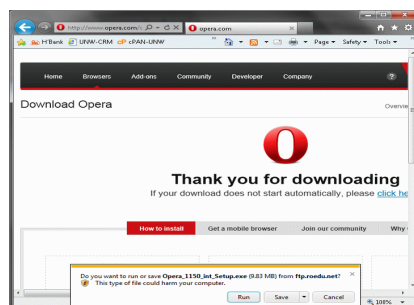
Una din cele mai bune caracteristici este unealta de screenshot, accesibilă prin click-dreapta, care poate captura o întreagă pagină web fără a fi nevoie de scroll. Această imagine odată preluată, ea este încărcată în serverele Mozilla, de unde se poate descărca timp de 14 zile.

Interfața este în întregime reprojctată, oferind un aspect mai curat, mai ordonat, cu animații subtile care cresc îmbunătățirea în performanță.



Toate elementele pentru securitate se pot găsi în meniul principal Options, în loc de a fi, cum erau, împrăștiate în diferite zone ale interfeței. De asemenea protecția anti-phishing și blocarea de pop-up-uri sunt activate în mod implicit. Lucrul cu parole este de asemenea simplu, nefiind necesară descărcarea unui administrator/manager de parole (password manager) separat.

Opera



Acest browser este dezvoltat în Oslo de către firma Opera Software, din 1996. Oferă browserul web, client de e-mail, știri, serviciu de chat IRC(Internet Relay Chat), client BitTorrent.

- se poate bloca conținutul (imagini, animație, bannere publicitare)
- permite previzualizarea informației atunci când mouse-ul se află deasupra unei pagini
- permite navigarea pe mai multe site-uri într-o singură fereastră

Browserul este foarte util în special atunci când conexiunile la internet sunt slabe sau de viteză mică.

Se lansează rapid, interfața pentru utilizatori este simplă, clară, și face aproape tot ce fac și navigatoarele cu care este în competiție.

Caracteristica Turbo este utilă pentru comprimarea traficului web, rutarea acestuia prin serverele Opera. Acest lucru este important atunci când legătura la internet este de tip dial-up, când acoperirea rețelei este proastă sau când internetul merge pur și simplu prost.

Poate fi ușor controlat și din tastatură sau gesturi mouse, sau control de voce. Acestea sunt utile pentru utilizatori cu handicap, sau copii.

Browserul rulează pe Windows, Linux, macOS, iOS, Android.

Alte browsere existente:

- Internet Explorer

- Microsoft Edge
- Safari
- Epic Privacy (de la Hidden Reflex)
- Comodo Dragon Internet (bazat pe Chromium)
- Tor

Conform unui studiu efectuat în 2018 de către Alice Woods de la firma Esolutions, niciunul din browsere nu este perfect, unele oferă siguranță față de malware, altele au setări foarte bune de confidențialitate, sau sunt prietenoase și ușor de folosit.

Ierarhia lui Alice este următoarea, din perspectiva siguranței browserului:

1. Google Chrome
2. Tor
3. Epic Privacy Browser
4. Microsoft Edge
5. Opera

Conform unor statistici din 2005, ca motoare de căutare folosite în întreaga lume, Google reprezenta 51%, Yahoo 24%, MSN 13%, AOL 5%, Ask Jeeves 5%, altele 2%.

Tot din punctul de vedere al statisticilor, căutările pe Google erau în 1999 în număr de 3 milioane pe zi, ajungând în 2019 la $2 \cdot 10^{12}$ căutări pe zi, iar în prezent se presupune că a ajuns la circa 63000 căutări pe secundă, adică $5.5 \cdot 10^{12}$ căutări pe zi.

Google Chrome



Chrome este un browser de tip open source și este cel mai utilizat, fiind în prezent folosit pe piață într-un procent de 52.1%. Prima versiune apare în 2008, scopul creării acestui browser fiind necesitatea pentru îmbunătățirea vitezei, o mai bună securitate și

stabilitate, față de browserele web existente. Numele navigatorului este derivat de la interfața grafică.

Acest browser este util dacă sistemul dispune de suficiente resurse.

Ca și caracteristici de bază ar fi:

- Viteza
- Este expandabil la infinit
- Dispune de dezvoltări beta

Acest browser este puternic pentru că oferă multe opțiuni și poate fi ușor adaptat nevoilor utilizatorului. Este cel mai bun browser în prezent, dacă nu interesează protecția datelor și utilizarea unor cantități mari de resurse. Funcționează pe sisteme de operare de tip Windows, Mac, Linux, Android, iOS.

Dacă utilizatorul are cont Google, toate aplicațiile sunt legate în mod armonios și este foarte facil accesul la toate tipurile de date. Se pot sincroniza setările și bookmark-urile de pe calculatoare diferite sau alte dispozitive, datorită versiunilor mobile ale browserului. Se pot foarte ușor adăuga funcții sau extensii. După cum se prezintă mai jos, există o gamă foarte largă de opțiuni în Chrome Web Store.

Lucrul cu tab-uri este facil, acestea putând fi redimensionate în mod inteligent, fiecare tab este stocat într-o zonă diferită de memorie astfel încât, dacă vreuna este distrusă, acest lucru să nu afecteze restul setărilor.

Ca și design, Chrome este minimalist, astfel foarte ușor de folosit, accentul este pus pe paginile web și afișarea acestora. Acest browser are și posibilitatea de utilizatori multipli sau control parental.

Browserul Google Chrome este foarte eficient în actualizarea periodică a bazelor de date privind protecția împotriva înșelătoriei, adică phishing, precum și împotriva malware-ului, avertizând utilizatorii atunci când aceștia au intenția de a vizita o pagină unde pot exista probleme. Chrome pune la dispoziția utilizatorilor un API care este free, denumit Google Safe Browsing API, care ajută la navigarea în siguranță.

Sandboxing adaugă un strat extra de protecție și previne instalarea automată a softului de tip malware, instrucțiunile fiind incorporate în codul programului.

Browserul Chrome permite modul incognito pentru personalizarea manuală a preferințelor de confidențialitate. Totuși, pașii utilizatorilor sunt urmăriți și anume click-uri, cuvinte cheie, tipuri de site-uri vizitate.

În ce privește dezavantajele, se poate observa faptul că folosește foarte multe resurse, deci nu este foarte bun pentru calculatoare cu un număr limitat de RAMi. De asemenea nu te poți simți în siguranță în ceea ce privește informațiile pe care tu le cauți și le accesezi în timpul navigării.

Chrome permite autentificarea în doi pași, lucru care este posibil combinând intrarea în cont cu parolă împreună cu un cod pseudo-aleatoriu; pe telefon permite de asemenea login folosind amprenta.

Legat de informațiile personale la Google, se spune că „orice informații cu caracter personal trimise la Google sau stocate în Contul Google vor fi folosite și protejate în conformitate cu Politica de confidențialitate Google”. Rămâne de văzut ce presupune acest lucru.

Moduri pentru browser

Nu este necesar să oferi informații cu caracter personal pentru a folosi Chrome, însă în Chrome există diferite moduri cu ajutorul cărora poți să îți modifici sau să îți îmbunătățești experiența de navigare. Politica de confidențialitate este diferită în funcție de modul pe care îl folosești.

Modul de bază al browserului

Modul de bază al browserului stochează informațiile local pe sistemul tău. Acestea pot să includă:

- informații din istoricul de navigare. De exemplu, Chrome stochează adresele URL ale paginilor pe care le accesezi, o copie cache a textului, a imaginilor și a altor resurse din paginile respective, iar dacă este activată funcția de predicție a acțiunilor în rețea, stochează și o listă a unora dintre adresele IP conectate din paginile respective;
 - informații cu caracter personal și parole, pentru a te ajuta să completezi formulare sau să te conectezi pe site-uri pe care le accesezi;
 - listă a permisiunilor pe care le-ai acordat site-urilor;
 - capturi de ecran miniatură ale paginilor pe care le accesezi cel mai frecvent;
 - cookie-uri sau date de pe site-urile pe care le accesezi;
 - date salvate de suplimente;
 - o evidență a materialelor descărcate de tine de pe site-uri.
- Aceste acțiuni se pot gestiona în mai multe moduri:

- se pot șterge informațiile din istoricul de navigare;
- se pot șterge cookie-urile și datele privind site-urile accesând caseta de dialog Cookie, iar datele despre site-urile vizitate de la `chrome://settings/clearBrowserData`;
- Chrome poate fi împiedicat să accepte cookie-uri de la Google sau de pe alte site-uri.
- Pot fi să examineze parolele salvate în setările Chrome.
- Se pot vedea și gestiona informațiile de completare automată stocate.
- Informațiile personale stocate de Chrome nu vor fi trimise la Google decât dacă utilizatorul optează pentru stocarea datelor respective în Contul Google conectându-se la Chrome. Atunci când se conectează, se activează funcția Chrome de sincronizare .

Funcții Chrome și setări

Preluarea în avans. Pentru a încărca mai rapid pagini web, Chrome are o setare care poate să caute adresele IP ale linkurilor de pe o pagină web și din conexiuni de rețea deschise. Și site-urile și aplicațiile Android pot să solicite browserului să încarce în avans paginile pe care este posibil să le accesezi în continuare. Solicitățile de încărcare anticipată din aplicațiile Android sunt controlate de aceeași setare ca predicțiile inițiate de Chrome. Însă solicitările de încărcare anticipată de pe site-uri sunt onorate întotdeauna, indiferent dacă funcția de predicție în rețea din Chrome este activată sau nu. Dacă se solicită redarea anticipată, fie de către Chrome, fie de către un site sau o aplicație, site-ul încărcat anticipat poate să seteze și să își citească propriile cookie-uri, ca și când l-ai fi accesat, chiar dacă până la urmă nu accesezi pagina preluată anticipat.

Locația. Pentru a primi mai multe informații relevante din punct de vedere geografic, Chrome îți oferă opțiunea să permiți accesul unui site la locația ta. Chrome nu va permite unui site să îți acceseze locația fără permisiunea ta. Cu toate acestea, pe dispozitive mobile, Chrome permite automat accesul motorului de căutare prestabilit la locația ta dacă aplicația Chrome are permisiunea să îți acceseze locația și dacă nu ai blocat localizarea geografică pentru site-ul asociat. Chrome folosește Serviciile de localizare Google pentru a-ți estima locația. Informațiile pe care Chrome le trimite Serviciilor de localizare Google pot să includă:

- routerele Wi-Fi cele mai apropiate de tine;
- ID-urile turnurilor de telefonie mobilă cele mai apropiate de tine;
- intensitatea semnalului Wi-Fi sau de telefonie mobilă;
- adresa IP atribuită în prezent dispozitivului tău.

Google nu deține controlul asupra site-urilor terță parte, nici asupra politicilor de confidențialitate ale acestora. Prin urmare, fii atent(ă) când permiți accesul unui site la locația ta.

Actualizări. Chrome trimite periodic informații la Google pentru a căuta actualizări, pentru a primi starea conexiunii, pentru a valida ora actuală și pentru a estima numărul de utilizatori activi.

Funcțiile de căutare. Dacă Google este motorul de căutare prestabilit, Chrome contactează Google când începi să cauți sau când treci la altă rețea, pentru ca tu să obții cea mai bună adresă web locală pentru trimiterea termenilor de căutare. Dacă te-ai conectat pe un site Google sau la Chrome și Google este motorul tău de căutare prestabilit, căutările efectuate de tine folosind bara de adrese din Chrome sunt stocate în Contul Google.

Serviciul de predicție a căutărilor. Pentru a te ajuta să găsești informații mai rapid, Chrome folosește serviciul de predicții oferit de motorul de căutare prestabilit ca să ofere completări probabile ale textului pe care îl introduci. Când cauți folosind bara de adrese din Chrome, caracterele pe care le introduci (chiar dacă nu ai apăsat încă „enter”) sunt trimise motorului tău de căutare prestabilit. Dacă Google este motorul tău de căutare prestabilit, predicțiile sunt bazate pe istoricul căutărilor tale, pe subiecte care au legătură cu ceea ce introduci și pe ceea ce cauți alte persoane. Află mai multe. Predicțiile pot fi bazate și pe istoricul de navigare.

Asistența la navigare. Când nu te poți conecta la pagina web, poți să primești sugestii pentru alte pagini similare cu cea pe care încerci să o accesezi. Pentru a-ți oferi sugestii, Chrome trimite la Google adresa URL a paginii pe care încerci să o accesezi.

Completarea automată și gestionarea parolelor. Chrome trimite la Google informații limitate și anonime despre formularele web pe care le întâlnești, inclusiv o adresă URL fragmentată a paginii web și detalii despre structura formularului, pentru ca Google să își poată

îmbunătăți serviciile de completare automată și de gestionare a parolelor.

Plățile. Dacă te-ai conectat la browserul Chrome și ai carduri de credit stocate în contul Google Payments, Chrome îți va oferi opțiunea să completezi datele cardurilor respective în formulare web. În plus, dacă introduci un card de credit nou într-un formular web, Chrome va oferi opțiunea de a salva cardul de credit și informațiile de facturare asociate acestuia în contul Google Payments. Dacă folosești un card din Google Payments sau alegi să îți salvezi cardul de credit în contul Google Payments în vederea utilizării viitoare, Chrome va culege informații despre computerul tău și le va trimite la Google Payments pentru a te proteja împotriva fraudelor. Dacă respectivul comerciant acceptă, poți folosi Chrome pe Android pentru a plăti prin Android Pay.

Limba. Pentru a-ți personaliza experiența de navigare în baza limbilor în care preferi să citești, Chrome va ține o evidență a limbilor folosite cel mai frecvent pe site-urile pe care le-ai accesat. Această preferință de limbă va fi trimisă la Google pentru a-ți personaliza experiența în Chrome. Dacă te-ai conectat la Chrome, acest profil de limbă va fi asociat Contului tău Google și, dacă incluzi istoricul Chrome în Activitatea de pe web și din aplicații Google, profilul poate fi folosit pentru a-ți personaliza experiența în alte produse Google.

Aplicațiile web pe Android. Pe dispozitivele Android, dacă selectezi „adaugă pe ecranul de pornire” pentru un site care a fost optimizat pentru performanță rapidă și fiabilă pe dispozitivele mobile, Chrome va folosi un server Google pentru a crea un pachet Android nativ pentru site-ul respectiv pe dispozitivul tău. Cu ajutorul pachetului Android poți să interacționezi cu aplicația web așa cum ai interacționa cu o aplicație Android. De exemplu, aplicația web va apărea în lista ta de aplicații instalate.

Statisticile de utilizare și rapoartele de blocare. În mod prestabilit, statisticile de utilizare și rapoartele de blocare sunt trimise la Google pentru a ne ajuta să ne îmbunătățim produsele. Statisticile de utilizare conțin informații cum ar fi preferințele, clicurile pe butoane și utilizarea memoriei. În general, statisticile de utilizare nu includ adrese URL de pagini web sau informații cu caracter personal, însă, dacă te-ai conectat la Chrome și îți sincronizezi istoricul de navigare

În Contul Google fără să folosești o expresie de acces pentru sincronizare, statisticile de utilizare Chrome includ informații despre paginile web pe care le accesezi și utilizarea acestora. De exemplu, este posibil să culegem statistici pentru a identifica paginile web care se încarcă lent. Folosim aceste informații pentru a ne îmbunătăți produsele și serviciile și pentru a le oferi dezvoltatorilor web informațiile necesare pentru a-și îmbunătăți paginile. Rapoartele de blocare conțin informații despre sistem la momentul blocării și pot să conțină adrese URL ale paginilor web sau informații cu caracter personal, în funcție de ce se întâmpla la momentul declanșării raportului de blocare. Putem să permitem accesul la informații agregate, care nu identifică personal utilizatorii, pentru public sau pentru parteneri, de exemplu, pentru editori, advertiseri sau dezvoltatori web. Poți să modifice oricând setările privind trimiterea statisticilor de utilizare și a rapoartelor de blocare la Google. Află mai multe. Dacă ai aplicații Google Play activate pe Chromebook, iar statisticile de utilizare Chrome sunt activate, la Google se trimit și date de diagnosticare și privind utilizarea Android.

Licențe media. Unele site-uri pot să creeze conținutul media ca protecție împotriva accesării și copierii neautorizate. Pentru site-urile cu HTML5, acest schimb de chei are loc prin API-ul Encrypted Media Extensions. În procesul de permitere a accesului la acest conținut media, se pot stoca local identificatori de sesiune și licențe. Utilizatorul poate să șteargă acești identificatori din Chrome folosind comanda Șterge datele de navigare, având activată opțiunea „Licențe media”. Pentru site-urile care folosesc Adobe Flash Access, browserul Chrome pentru sistemul de operare Windows sau Chrome oferă un identificator unic partenerilor de conținut și site-urilor. Identificatorul este stocat în sistemul tău. Poți să refuzi acest acces din Setări privind conținutul, Conținut protejat și să resetezi ID-ul folosind comanda Șterge datele de navigare, având activată opțiunea „Licențe media”. Dacă accesezi conținut HD în sistemul de operare Chrome, este posibil ca un furnizor de conținut să solicite un certificat de la Chrome pentru a confirma eligibilitatea dispozitivului. Pentru a confirma dispozitivul, Chromebookul va trimite date despre capacitățile sale hardware site-ului și va folosi Accesul verificat pentru a certifica protejarea cheilor sale criptografice prin hardware Chrome.

Alte servicii Google. Această notificare descrie serviciile Google activate în mod prestabilit în Chrome. În plus, Chrome poate să ofere alte servicii web Google. De exemplu, dacă accesezi o pagină în altă limbă, Chrome va oferi trimiterea textului la Google pentru traducere. Când începi să folosești serviciile respective, vei fi notificat(ă) privind opțiunile de control ale acestora. Informații suplimentare poți să găsești în Documentația privind confidențialitatea Google Chrome.

Identificatori din Chrome. Chrome include o serie de identificatori necesari pentru procedurile funcțiilor. De exemplu, dacă folosești mesageria push, se creează un identificator pentru ca tu să primești notificările. Când este posibil, folosim identificatori care nu sunt unici și eliminăm identificatorii când aceștia nu mai sunt necesari.

Urmărirea instalărilor. Fiecare copie a versiunii pentru desktop Windows a browserului Chrome include un număr de instalare temporar, generat aleatoriu, trimis la Google când instalezi și folosești Chrome pentru prima oară. Cu ajutorul acestui identificator temporar putem să estimăm numărul de browsere instalate. Acesta va fi șters la prima actualizare Chrome. Versiunea mobilă de Chrome folosește permanent o variantă a identificatorului dispozitivului pentru a urmări numărul de instalări Chrome.

Urmărirea promoțiilor. Pentru a urmări reușita campaniilor promoționale, Chrome generează un indicativ unic trimis la Google când instalezi și folosești browserul pentru prima oară. În plus, dacă ai primit sau ai reactivat copia versiunii pentru desktop a browserului Chrome în cadrul unei campanii promoționale, iar Google este motorul de căutare prestabilit, căutările din caseta polivalentă includ o etichetă promoțională care nu este unică. Toate versiunile pentru mobil ale browserului Chrome includ o etichetă promoțională care nu este unică în căutările din caseta polivalentă. Este posibil ca sistemul de operare Chrome să trimită periodic la Google o etichetă promoțională care nu este unică (inclusiv în timpul configurării inițiale) și când se caută folosind Google.

Testările. Uneori desfășurăm testări limitate ale funcțiilor noi. Chrome include un număr de bază selectat aleatoriu la prima rulare pentru a atribui browserele unor grupuri experimentale. De asemenea, experimentele pot fi limitate în funcție de țară (stabilită în funcție de adresa ta IP), de sistemul de operare, de versiunea

Chrome și de alți parametri. Toate solicitările trimise la Google includ o listă a testărilor active în prezent în instalarea ta Chrome.

Modul Chrome conectat

- Când te conectezi la browserul Chrome sau la un Chromebook folosind Contul Google, datele tale de navigare personale sunt salvate pe serverele Google și sincronizate cu contul tău. Acest tip de informații poate să includă:
- istoricul de navigare,
- marcaje,
- file,
- parole și informații de Completare automată,
- alte setări ale browserului, cum ar fi extensiile instalate.

Aceste setări sunt încărcate automat pentru tine de fiecare dată când te conectezi la Chrome de pe alte computere sau dispozitive. Pentru a personaliza informațiile specifice pe care le sincronizezi, folosește meniul „Setări”. Află mai multe. Poți vedea cantitatea de date Chrome stocate în Contul Google și o poți gestiona din Tabloul de bord Sincronizare Chrome. În Tabloul de bord, cu excepția Conturilor Google create prin Family Link, poți să dezactivezi complet sincronizarea și să ștergi toate datele asociate de pe serverele Google. Află mai multe. Copiii care au Conturi Google create în Family Link trebuie să se conecteze, iar Sincronizarea Chrome nu poate fi dezactivată, deoarece oferă funcții de gestionare parentală, cum ar fi restricțiile privind site-urile. Cu toate acestea, copiii cu astfel de conturi pot să-și șteargă datele și să dezactiveze sincronizarea pentru majoritatea tipurilor de date. Află mai multe. Notificarea privind confidențialitatea pentru Conturile Google create în Family Link se aplică pentru datele Sincronizare Chrome stocate în conturile respective.

Cum gestionează Chrome informațiile tale când ești conectat

Când sincronizezi Chrome cu Contul Google, folosim datele tale de navigare pentru a-ți îmbunătăți și a-ți personaliza experiența Chrome. Îți poți personaliza experiența și în alte produse Google, dacă permiți ca istoricul tău Chrome să fie inclus în Activitatea de pe web și din aplicații Google.

Poți să schimbi această setare din pagina Istoricul contului sau poți să îți gestionezi datele privateoricând dorești. Dacă nu îți folosești datele Chrome pentru a-ți personaliza experiența Google în afara Chrome, Google va folosi datele tale Chrome numai după ce sunt

anonimizate și agregate cu datele altor utilizatori. Google folosește aceste date pentru a dezvolta funcții, produse și servicii noi și pentru a îmbunătăți calitatea generală a produselor și serviciilor existente. Dacă vrei să folosești serviciul cloud Google pentru stocarea și sincronizarea datelor Chrome, însă nu vrei ca Google să acceseze datele respective, poți să criptezi toate datele sincronizate folosind propria ta expresie de acces.

Modul incognito și modul pentru invitați

Poți să limitezi informațiile stocate de Chrome în sistemul tău folosind modul incognito sau modul pentru invitați. În aceste moduri, Chrome nu va stoca anumite informații, cum ar fi:

- informațiile de bază din istoricul de navigare, cum ar fi adresele URL, textul memorat în cache al paginii sau adresele IP ale paginilor conectate din site-urile pe care le accesezi;
- capturile de ecran ale paginilor pe care le accesezi;
- evidențe ale descărcărilor tale, deși fișierele pe care le descarci vor fi în continuare stocate altundeva, pe computer sau pe dispozitiv.

Cum gestionează Chrome informațiile tale incognito și despre invitați **Cookie-urile**. Chrome nu va permite accesul la cookie-urile existente site-urilor pe care le accesezi incognito sau în modul pentru invitați. Site-urile pot să plaseze cookie-uri noi în sistemul tău când folosești aceste moduri, însă acestea vor fi stocate și transmise numai până când închizi și ultima fereastră din modul incognito sau pentru invitați.

Modificările privind configurația browserului. Când modifizi configurația browserului, de exemplu, adăugând un marcaj pentru o pagină web sau schimbând setările, aceste informații sunt salvate. Modificările nu sunt afectate de modul incognito sau de cel pentru invitați.

Permisiunile. Permisiunile pe care le acorzi în modul incognito nu sunt salvate în profilul tău actual.

Informațiile de profil. În modul incognito, vei avea în continuare acces la informații din profilul tău existent, cum ar fi sugestiile bazate pe istoricul de navigare și parolele salvate, în timp ce navighezi
Gestionarea utilizatorilor pentru utilizarea Chrome personală

Poți să configurezi versiuni personalizate de Chrome pentru utilizatori care folosesc același dispozitiv sau același computer. Reține că orice persoană care are acces la dispozitivul tău poate să vadă toate informațiile din toate profilurile. Pentru a-ți proteja cu adevărat datele astfel încât alții să nu le poată vedea, folosește conturile de utilizator încorporate din sistemul de operare.

Gestionarea utilizatorilor în Chrome for Enterprise

Anumite browsere Chrome sau Chromebookuri sunt gestionate de o școală sau de o companie. În astfel de cazuri, administratorul poate să aplice politici în browser sau pe Chromebook. Chrome contactează Google pentru a verifica existența unor astfel de politici când un utilizator se conectează pentru prima oară la Chrome sau când începe să folosească browserul fără să se conecteze (cu excepția modului pentru invitați). Chrome verifică periodic dacă există actualizări ale acestor politici.

Un administrator poate să configureze o politică pentru raportarea stării și a activității pentru Chrome, incluzând informații despre locație în cazul dispozitivelor cu sistemul de operare Chrome. Administratorii dispozitivului tău pot avea capacitatea să acceseze, să monitorizeze sau să divulge date accesate de pe dispozitivul tău gestionat.

Practici de Navigare sigură

Google Chrome și anumite browsere terță parte, cum ar fi unele versiuni de Mozilla Firefox și Safari de la Apple includ funcția Navigare sigură de la Google. Folosind Navigarea sigură, informațiile despre site-urile suspecte sunt trimise și primite între browserul pe care îl folosești și serverele Google.

Modul de funcționare al funcției de Navigare sigură

Browserul contactează serverele Google periodic pentru a descărca cea mai recentă listă „Navigare sigură”, cu site-urile despre care se știe că includ phishing și programe malware. Cea mai recentă copie a listei este stocată local, pe sistemul tău. Google nu culege niciun fel de informații din cont, nici alte informații care te identifică personal în cadrul acestui contact. Cu toate acestea, primește informații standard de jurnal, inclusiv o adresă IP și cookie-uri.

Fiecare site pe care îl accesezi este căutat în lista Navigare sigură din sistemul tău. Dacă există o potrivire, browserul trimite la Google o copie trunchiată a adresei URL a site-ului, pentru ca Google să poată trimite mai multe informații browserului. Google nu poate să

stabilească adresa URL pornind de la aceste informații. Află mai multe.

Următoarele funcții Navigare sigură sunt specifice pentru Chrome.

- Unele versiuni Chrome includ tehnologie Navigare sigură care poate să identifice potențialele site-uri periculoase și potențialele tipuri de fișiere periculoase necunoscute încă de Google. Adresa URL completă a site-ului sau a potențialului fișier periculos poate fi trimisă la Google. Va fi utilă pentru a se stabili dacă site-ul sau fișierul este periculos.
- Chrome folosește tehnologia Navigare sigură pentru a scana computerul periodic, cu scopul de a detecta software-ul nedorit care te împiedică să schimbi setările sau care afectează în alt mod securitatea și stabilitatea browserului. Află mai multe. Dacă se detectează astfel de software, Chrome poate să îți ofere opțiunea să descarci Chrome Cleanup Tool pentru a-l elimina.
- Când accesezi un site care pare să conțină programe malware sau când Chrome detectează software nedorit pe computer, poți alege să trimiți date suplimentare pentru a îmbunătăți Navigarea sigură. Află mai multe.
- Dacă folosești managerul de parole din Chrome, Navigarea sigură solicită informații de la Google când introduci o parolă salvată pe o pagină neobișnuită, ca să te protejeze de phishing. În plus, Navigarea sigură îți protejează parola Contului Google. Dacă o introduci pe un site care pare de phishing, Chrome îți va solicita să îți schimbi parola contului Google. Dacă sincronizezi istoricul de navigare, Google îți va semnala și Contul Google personal ca fiind probabil compromis prin phishing.
- Dacă folosești Navigarea sigură și sincronizezi istoricul de navigare Chrome cu Contul Google, atunci, pentru a îmbunătăți siguranța și utilitatea permisiunilor pentru funcția web, Chrome poate să raporteze anonim domeniile cărora le acorzi, le refuzi sau le revoci permisiunile sau pentru care ignori ori închizi solicitările de permisiuni.

Poți oricând să dezactivezi funcția Navigare sigură din Chrome.

Politicile de confidențialitate ale aplicațiilor, extensiilor, temelor, serviciilor și ale altor suplimente

Poți să folosești aplicații, extensii, teme, servicii și alte suplimente în Chrome, inclusiv unele care pot fi preinstalate sau integrate cu

Chrome. Suplimentele dezvoltate și furnizate de Google pot comunica cu serverele Google și sunt supuse Politicii de confidențialitate Google, cu excepția cazului când există alte prevederi. Responsabilitatea pentru suplimentele dezvoltate și oferite de alte părți revine creatorilor acestora și se pot aplica politici de confidențialitate diferite.

Gestionarea suplimentelor

- Înainte de a instala un supliment, îți recomandăm să examinezi permisiunile solicitate. Suplimentele pot avea diferite permisiuni, de exemplu:
- să stocheze, să acceseze și să trimită date stocate local sau în contul tău Google Drive;
- să vadă și să acceseze conținut de pe site-urile pe care le vizitezi;
- să folosească notificări trimise prin serverele Google.
- Chrome poate să interacționeze cu suplimentele în câteva moduri diferite:
- căutând actualizări;
- descărcând și instalând actualizări;
- trimițând indicatori de utilizare la Google despre suplimente.

Pentru anumite suplimente poate fi necesar accesul la un identificator unic pentru administrarea drepturilor digitale sau pentru livrarea mesajelor push. Poți să dezactivezi utilizarea identificatorilor eliminând suplimentul din Chrome.

Din când în când, Google poate descoperi un supliment care constituie o amenințare de securitate, care încalcă termenii Magazinului web Chrome sau alte acorduri legale, legi, reglementări sau politici. Chrome descarcă periodic o listă a acestor suplimente periculoase, pentru a le dezactiva de la distanță sau pentru a le elimina din sistemul tău.

Cookie-uri

Un cookie este un mic fișier care conține un șir de caractere, trimis computerului tău când accesezi un site. Când accesezi din nou site-ul, cookie-ul îți permite acestuia să îți recunoască browserul.

Cookie-urile pot stoca preferințele utilizatorului, precum și alte informații. Poți reconfigura browserul astfel încât să respingă toate cookie-urile sau să te informeze când este trimis un cookie. Cu toate acestea, este posibil ca anumite funcții sau servicii ale site-urilor să nu funcționeze corespunzător fără cookie-uri. Pe alte platforme unde cookie-urile nu sunt disponibile sau aplicabile, se folosesc alte

tehnologii în scopuri similare cu cele ale cookie-urilor. Un astfel de exemplu îl constituie ID-ul publicitar disponibil pe dispozitivele mobile Android.

Jurnalul de server

La fel ca în cazul majorității site-urilor, serverele noastre înregistrează automat solicitările de pagini efectuate când un utilizator ne accesează site-urile. Aceste „jurnale de server” includ, de obicei, solicitarea ta web, adresa IP, tipul de browser, limba browserului, data și ora solicitării și unul sau mai multe cookie-uri care îți pot identifica în mod unic browserul.

Iată un exemplu de intrare tipică în jurnal. Termenul căutat este „mașini”, apoi urmează o **detaliere a părților intrării în jurnal**:

123.45.67.89 - 25/Mar/2003 10:15:32 -
https://www.google.com/search?q=mașini -Firefox 1.0.7;
Windows NT 5.1 - 740674ce2123e969

- **123.45.67.89 este adresa de protocol de internet atribuită utilizatorului de ISP-ul său. În funcție de serviciul utilizatorului, furnizorul de servicii îi poate atribui acestuia o adresă diferită de fiecare dată când se conectează la internet.**
- **25/Mar/2003 10:15:32 este data și ora la care s-a folosit termenul de căutare;**
- **https://www.google.com/search?q=mașini este adresa URL solicitată, care include termenul de căutare;**
- **Firefox 1.0.7; Windows NT 5.1 este browserul și sistemul de operare folosit; iar**
- **740674ce2123a969 este ID-ul unic al cookie-ului atribuit special acestui computer prima oară când a accesat Google. (Cookie-urile pot fi șterse de utilizatori. Dacă după ultima accesarea a site-ului Google, utilizatorul a șters cookie-ul din computer, atunci acesta va fi ID-ul unic de cookie atribuit utilizatorului la următoarea accesare a site-ului Google de pe respectivul computer)**

Extensii ale Google Chrome

Observație: Se enumeră în continuare doar câteva exemple de posibile extensii și instrumente ale acestui browser, pentru a evidenția posibilitățile în permanentă dezvoltare care există.

Google Keep

Turn off the lights (stinge lumina)

Streak CRM pentru Gmail

IMTranslator

Stylus

Explain&Send Screenshots(Fotografiaza si explică)

Office Online

Momentum – personal dashboard-to do, weather, inspiration

FireShot – printscreen care permite capturarea,editarea, salvarea sau trimiterea imaginii capturate

Mega- secure cloud storage

E-mail tracking- pentru Gmail si Google Inbox

ScreenCast- records screen as video – permite adnotări pe pagină, blurarea informațiilor neneesare precum și share

Earth View – la fiecare nou tab deschis, se prezintă o imagine din satelit de pe Pământ

Instrumente Chrome

Data saver – economizor de date- sunt folosite serverele google pentru ca paginile ce urmează să fie descărcate, să fie în prealabil comprimate; acest lucru nu este posibil pentru paginile incognito sau deschise în mod https. Prin click pe „delatii” poți afla cât de mult sunt consumate resursele de date

Google dictionary – arată definiții ale cuvintelor, în timpul navigării

Great suspender – „suspendă” activitățile din tab-urile pe care nu le folosești la un moment dat, dar sunt deschise; adică activitatea acestora este lăsată în background

Speedtest

Zoom – aplicație pentru video conferințe

GoToMeeting – planificator, planner

Calendar

Assistant to - asistent

Ginger- permite verificarea și corectarea textelor din limba engleză (spelling, grammar checker) având funcții legate de gramatică, structură, ortografie, punctuație, sinonime, traducere și cuvinte de dicționar. Această extensie este utilă atât pentru perfecționarea comunicării de tip business cât și pentru corectitudinea descrierilor și a altor texte din site-urile create

Speak it- transformă textul în sunet, astfel încât îți poate economisi timpul; de exemplu poți asculta textul când ești pe drum, în mașină

Hoover Zoom – mărește thumbnails atunci când se trece cu mouse-ul peste ele

Mercury Reader – păstrează textul „curat” pentru a fi citit, adică elimină reclamele și orice alte adăugiri care ar putea exista pe lângă text

PrintFriendly

Darkness – colector de teme vizuale dark pentru Facebook, google, YouTube, Gmail, Google Docs, Reddit, Twitter etc

Forest- aplicație care să permită să lucrezi eficient, să te concentrezi doar pe lucrul tău; se consideră că te salvează de la dependența de internet. Se pornește de la plantarea unei semințe în pădure, care se va transforma într-un copac în următoarele 30 de minute. Copacii pot fi share-uiti cu prietenii. În paralel, ai creat o listă neagră cu site-uri care trebuie evitate în timpul lucrului, astfel încât dacă nu rezisti tentației de a accesa acele pagini din blacklist, copacul va muri. Această aplicație este utilă nu doar pentru înlăturarea dependenței de internet, dar și pentru cultivarea autodisciplinii, pentru realizarea unei structuri personale de timp pe care fiecare o planifică cum îi este mai util, eficientizarea lucrului pe intervale de 30 de minute.

Google academic

Password Alert

What runs- descoperă care sunt aplicațiile și mecanismele care fac un site să funcționeze, să ruleze. Prezintă unelte de studiu analitic, plug-ins wordpress, fonturi, unelte de dezvoltatori, alte servicii. Cu această aplicație se pot urmări site-uri, permițându-ți astfel să afli ce tehnologii folosesc aceste pagini și la care instrumente se renunță. Orice tehnologie folosită la un site, lasă urme care se pot detecta. Algoritmul din această aplicație recunoaște anumite tipare care rulează. Spre deosebire de alte aplicații similare (Wappalyzer, BuiltWith, Datanyze, Ghostery) aceasta nu îngreunează mersul, activitatea browser-ului, are acuratețe mai mare de detecție și recunoaște și tehnologii de ultimă generație. De asemenea detectarea de plugins din wordpress, teme folosite pe site-uri, fonturi, aceste aspecte nu sunt recunoscute de către celelalte aplicații mai vechi.

OneTab – reduce memoria până la 95% și ordonează filele

Tab Resize- reorganizează tab-urile

NewTabRedirect

Tabs Oultiner

Tab Snooze

Session Buddy

Boomerang – funcționează pentru gmail; mesajele se pot programa ca să fie expediate mai târziu, chiar dacă nu ești online; se poate urmări răspunsul prin tracking; se pot planifica mesaje de reminder; notificare atunci când mesajul este citit

Sticky Notes

Multi Highlight

WhatRuns -

Captură de ecran – diferite aplicații care permit captura de ecran: One Note, Screencastify, Full Page Screen Capture, Nimbus, Diigo Web Collector, PicMonkey

Extensii artistice

Color Zilla

ColorPick

Sketch Pad

Musixmatch – catalog de lyrics pentru video-uri de pe youtube

Sumo Paint

Color Tab

Aplicații de socializare

Hangouts – combină conversațiile tip text cu fotografiile, emoticons sau apel video gratuit; funcțional pe computer, sisteme de operare de tip Android sau Apple; funcționează pe grup de maxim 10 persoane

Buton `+1` - este pentru recomandarea unei pagini web, care merită să fie accesată de persoanele din contactele personale sau alți utilizatori. Această extensie permite ca click-urile de tip `+1` să devină publice, apoi se pot distribui pe google, se pot face comentarii și se poate face share(distribuție)

Chrome IG Story – permite ca story-ul de pe Instagram al prietenilor să fie adăugat informațiilor pe care tu le afișezi pe Instagram; astfel se pot vedea story de la persoane pe care nu le urmărești

SocialBlade – arată diferite statistici raportate la YouTube, TwitchTV, Twitter, Instagram; prezintă o clasificare a canalului youtube despre cât este de vizitat, arată membrii înscriși, vizitatori pe zile sau pe lună, estimează posibilul câștig lunar al canalului, arată diverse tag-uri folosite de video-uri

Chat sub Chrome

Bitmoji

MightyText

Viber

MySMS

SMS din gmail sau facebook

Jocuri

Chrome-book- este un notebook pe care nu rulează Windows, ci sistemul de operare de la Google, Chrome OS. Notebook= computer portabil cu ecrane de 15-21 inch, dotate cu unitate optică. Rezoluția ecranului ajunge până la 1650x1050px sau chiar fullHD(1920x1080px) la ecrane peste 17 inch. Autonomia bateriei unui netbook atinge un interval orar de 9-13 ore. Aceste Chrome-book-uri funcționează neapărat cu conexiune la internet, deoarece majoritatea aplicațiilor și documentelor sunt stocate în cloud. Ca urmare, nu necesită un spațiu mare de stocare, deci nu au nevoie de memorie mare. Este eficientă acționarea aplicațiilor cu contul Google, lucrul acestor dispozitive este optimizat pentru aplicații Google. În aceste situații, softuri clasice precum Microsoft sau Adobe, nu rulează pe aceste notebook-uri, dar pot fi rulate online în versiuni gratuite, sau pot fi înlocuite aceste programe cu servicii Google.

Memoria ram standard este de 2-4GB dar există și modele cu 4GB. Memoria de stocare, cum spuneam, nu este foarte mare deoarece se mizează pe stocarea în Google Cloud, astfel că ea ajunge de la 16GB, la 32-64GB sau chiar până la 128-512GB, dar poate fi mărită dacă există slot de card SD.

Google Suite

Google Cloud

Platforma google Cloud, lansată în 7 aprilie 2008, este o mulțime de servicii oferite de Google pentru găzduire în cloud computing, punând la dispoziție 10Terrabiți pe secundă, astfel încât accesul la date este foarte rapid. Prin Cloud Hosting, se realizează accesul la rețeaua de servere care lucrează împreună, cu viteză mare de încărcare; dacă unul din servere are vreo problemă, toate aplicațiile tip e-mail, web, ftp, vor trece să ruleze pe alt server. Aceste lucruri sunt realizate prin servere fizice dar și prin mașini virtuale dispuse pe tot globul, accesibile din locațiile Google.

John Batelle: Fenomenul Google, Editura Orizonturi, București 2005

<https://www.w3.org>

www.techradar.com

<https://www.smartinsights.com>

<http://www.invata-programare.ro>

<http://adesoft.ro>

mozilla.org

<https://www.google.com>

<https://www.opera.com>

<https://www.toptenreviews.com/software/internet/best-internet-browser-software/>
<http://faravirus.ro/cel-mai-sigur-browser-din-2018/>
<https://www.w3.org>
<https://www.w3.org/WebCommerce/>
<https://www.w3.org/Payments/WG/>
<https://www.w3.org/Security/>
www.chrome.google.com
<http://www.calculator-service.ro>
www.laptopmag.com

V. Plăți online

Plățile electronice se referă efectuarea tranzacțiilor financiare prin mijloce electronice, precum servicii bancare online, carduri de credit sau de debit sau plăți mobile. Procesarea lor se face prin rețele electronice cum ar fi Internetul și pentru realizarea acestora nu este nevoie de utilizarea de numerar sau cec fizic.

Cele mai utilizate forme de plăți electronice includ cardurile de credit și de debit, serviciile bancare online și plățile mobile. Cardurile de credit și de debit, precum Mastercard și Visa, sunt acceptate pe scară largă atât de comercianții fizici, cât și la cei online și oferă caracteristici de securitate suplimentare, cum ar fi tehnologia cu cip și detectarea fraudelor. Banca online a devenit, de asemenea, tot mai răspândită, multe bănci oferind clienților posibilitatea de a efectua plăți și de a transfera fonduri prin intermediul site-urilor web și al aplicațiilor mobile.

Odată cu creșterea tehnologiilor digitale, utilizarea plăților electronice a devenit preponderentă față de metodele tradiționale precum numerarul și cecurile. Piața globală de plăți electronice valora 87,8 miliarde de dolari în 2021 și este estimată să ajungă la 19,89 trilioane de dolari până în 2026. Piața a avut un venit de 3,53 trilioane de dolari în anul 2018 și se așteaptă să prezinte o rată de creștere compusă anuală ("Compound Annual Growth Rate – CAGR) de 24,4%.

Primul sistem de plată electronică a fost introdus în 1960, odată cu utilizarea bancomatelor și dezvoltarea benzii magnetice pe cardurile de credit și de debit. Acest lucru a permis retrageri de numerar și tranzacții simple la punctul de vânzare. În anul 1980 și 1990, utilizarea sistemelor de transfer electronic de fonduri

("electronic funds transfer" – EFT), cum ar fi tranzacțiile cu depozitul direct și casa de compensare automată ("automated clearing house" – ACH), a devenit tot mai răspândită. Aceste sisteme au permis transferul de fonduri între conturile bancare prin mijloace electronice.

În anii 2000, ascensiunea internetului și a comerțului electronic a dus la dezvoltarea sistemelor de plată online, precum PayPal. Aceste sisteme au permis transferul ușor și sigur de fonduri pe internet și au oferit o opțiune convenabilă pentru cumpărătorii online. Introducerea smartphone-urilor și a tehnologiei mobile la sfârșitul anilor 2000 și începutul anilor 2010 a dus la dezvoltarea plăților mobile, cum ar fi Apple Pay și Google Wallet. Aceste sisteme permit utilizatorilor să efectueze plăți folosind smartphone-urile lor, fie prin tehnologia de comunicare în câmp apropiat (NFC), fie prin aplicații mobile care se conectează la cardul de credit sau de debit al utilizatorului. În ultimii ani, utilizarea tehnologiei blockchain și a criptomonedelor, cum ar fi Bitcoin, a fost, de asemenea, în creștere. Criptomonedele sunt monede digitale sau virtuale care folosesc criptografie pentru securitate și funcționează independent de o bancă centrală. Deși este încă o tehnologie relativ nouă, se așteaptă ca utilizarea criptomonedelor pentru plăți să continue să crească în viitor.

Plățile electronice au suferit schimbări semnificative în ultimele decenii, odată cu adoptarea tot mai mare a tehnologiilor digitale și cererea de confort și securitate. Aceste schimbări au condus la dezvoltarea unei game largi de sisteme și tehnologii de plată electronică, fiecare adaptată nevoilor și cazurilor de utilizare specifice. Plățile electronice devin normale pentru tranzacțiile financiare, odată cu adoptarea tot mai mare a tehnologiilor digitale și cererea de confort și securitate. Astfel, este de așteptat ca piața să continue să crească pe măsură ce tehnologia avansează și apar noi forme de plăți electronice.

Avantaje și dezavantaje ale plăților online

Ca avantaje pentru plățile electronice putem menționa:

- Comoditate: plățile electronice pot fi efectuate de oriunde și în orice moment, ceea ce facilitează clienților să facă achiziții și să plătească facturile;
- Rapiditate: plățile electronice sunt de obicei procesate mult mai rapid decât metodele de plată tradiționale, acest lucru

este valabil mai ales pentru plățile online, care pot fi procesate aproape instantaneu;

- **Securitate:** plățile electronice pot fi mai sigure decât metodele de plată tradiționale, deoarece sunt de obicei criptate, ceea ce face dificilă interceptarea și utilizarea fraudatorilor;
- **Gestionarea datelor:** plățile electronice generează date care pot fi utilizate pentru analiză și raportare. Aceste date pot ajuta companiile să înțeleagă mai bine comportamentul și nevoile clienților lor, ceea ce, la rândul său, poate ajuta la îmbunătățirea serviciului pentru clienți și la creșterea vânzărilor;
- **Eficiente din punct de vedere al costurilor:** plățile electronice pot fi mai rentabile decât metodele de plată tradiționale, deoarece pot economisi bani companiilor pe costurile de imprimare, corespondență și procesare;
- **Acoperire sporită:** plățile electronice permit companiilor să ajungă la mai mulți clienți decât oricând, deoarece pot procesa plăți de oriunde în lume.

Dezavantajele plăților electronice:

- **Dependență de tehnologie:** plățile electronice se bazează pe tehnologie, ceea ce înseamnă că, dacă există o problemă cu sistemul, este posibil ca plățile să nu poată fi procesate;
- **Potențial de fraudă:** deși plățile electronice sunt în general mai sigure decât metodele tradiționale de plată, ele sunt totuși vulnerabile la fraudă și pot fi mai dificil de detectat și prevenit;
- **Acceptare limitată:** plățile electronice nu sunt acceptate de toți comercianții și este posibil ca unele persoane să nu aibă acces la tehnologia necesară pentru a efectua plăți electronice;
- **Anonimat limitat:** plățile electronice lasă o amprentă digitală, ceea ce înseamnă că tranzacțiile pot fi urmărite până la persoana care le-a făcut;
- **Taxe:** unele metode de plată electronică pot percepe comisioane pentru tranzacții, care se pot adăuga în timp;
- **Întreruperea serviciului:** plățile electronice pot fi întrerupte de defecțiuni ale rețelei, întreruperi de curent și alte probleme care pot perturba accesul la serviciile de plată.

Este de remarcat faptul că dezavantajele plăților electronice pot fi atenuate de măsurile și reglementările adecvate de securitate.

Cardurile de credit și de debit

Cele mai utilizate metode de plată electronică sunt:

- Cardurile de credit și de debit;
- Serviciile bancare online;
- Plățile mobile;
- Cardurile preplătite;
- Portofelele electronice;
- Cecurile electronice;
- Criptomonede.

Cardurile de credit și de debit sunt una dintre cele mai utilizate metode de plată electronică. Sunt emise de bănci și instituții financiare și sunt acceptate atât la comercianții fizici, cât și online. Cardurile de credit permit clienților să împrumute bani și să facă achiziții pe credit, în timp ce cardurile de debit sunt legate de contul de verificare sau de economii al clientului, iar fondurile sunt deduse direct din cont.

Pentru a utiliza un card de credit sau de debit pentru o plată electronică, clienții trebuie mai întâi să aibă un card emis de o bancă sau instituție financiară. Odată obținut cardul, clienții îl pot folosi pentru a face achiziții de la comercianții care acceptă plăți cu cardul de credit sau debit. Acest lucru se poate face prin glisarea sau introducerea cardului într-un cititor de carduri sau prin introducerea online a informațiilor cardului. Unul dintre principalele avantaje ale utilizării cardurilor de credit și de debit este confortul pe care îl oferă. Cardurile de credit și de debit sunt acceptate pe scară largă la comercianți, atât online, cât și offline, și permit clienților să facă achiziții fără a fi nevoiți să transporte numerar. În plus, cardurile de credit și de debit oferă caracteristici de securitate suplimentare, cum ar fi tehnologia cipului și detectarea fraudelor, care pot ajuta la protejarea împotriva tranzacțiilor neautorizate.

Cardurile de credit oferă, de asemenea, recompense sub formă de cashback, reduceri sau puncte de călătorie. Un alt avantaj al utilizării cardurilor de credit este că acestea pot ajuta clienții să-și construiască istoricul de credit și să-și îmbunătățească scorul de

credit, ceea ce poate face mai ușor să se califice pentru împrumuturi sau alte produse de credit în viitor .

Tehnologia cu bandă magnetică și tehnologia NFC (comunicare în câmp apropiat) sunt ambele utilizate în procesarea plăților pentru a permite clienților să efectueze plăți electronice folosind un card fizic sau un dispozitiv mobil. Cardurile cu bandă magnetică au o bandă de material magnetic pe spatele cardului care stochează informații, cum ar fi numerele cardului de credit sau numerele personale de identificare (PIN). Acestea sunt citite de un cititor de carduri, care folosește un cap magnetic pentru a citi informațiile stocate pe card. Aceste carduri sunt utilizate pe scară largă de zeci de ani, pentru plățile cu cardul de credit și debit.

Tehnologia cu bandă magnetică este tehnologia care este utilizată astăzi pe majoritatea cardurilor de credit și de debit. Stochează date pe o bandă magnetică de pe spatele cardului, care poate fi citită de un cititor de carduri atunci când cardul este trecut prin el. Cititorul de carduri comunică apoi cu procesatorul de plăți pentru a procesa tranzacția.

Tehnologia NFC

Tehnologia NFC este o tehnologie fără contact care permite comunicarea între dispozitive care sunt ținute apropiate, cum ar fi un dispozitiv mobil și un terminal de la punctul de vânzare. Când un client dorește să efectueze o plată, își ține dispozitivul mobil (care are un cip NFC) lângă un terminal de la punctul de vânzare. Terminalul citește apoi informațiile de pe cipul NFC al dispozitivului mobil, iar plata este procesată.

În timp ce tehnologia cu bandă magnetică este considerată a fi mai puțin sigură, mai puțin fiabilă și mai puțin convenabilă decât tehnologia NFC, este încă utilizată pe scară largă datorită acceptării sale largi de către comercianți și compatibilității cu infrastructura existentă. Pe măsură ce tehnologia NFC devine tot mai răspândită, ea poate înlocui în cele din urmă tehnologia cu bandă magnetică ca standard pentru plățile electronice.

Cardurile cu tehnologie NFC, pe de altă parte, folosesc tehnologia de radiofrecvență (RF) pentru a comunica cu un cititor de carduri. În loc să gliseze sau să introducă cardul, clientul pur și simplu ține cardul lângă cititorul de carduri. Tehnologia NFC este utilizată în cardurile de credit și debit fără contact, precum și în plățile mobile și portofelele mobile.

Una dintre principalele diferențe dintre cele două este nivelul lor de securitate. Cardurile cu bandă magnetică sunt considerate mai puțin sigure decât cardurile NFC, deoarece datele stocate pe banda magnetică sunt statice și pot fi ușor copiate sau ignorate de criminali. Cardurile NFC, pe de altă parte, folosesc date dinamice și sunt criptate, făcându-le mai dificil de trecut sau copiat. În plus, cardurile NFC au, de asemenea, un interval de citire mai scurt, ceea ce îngreunează interceptarea comunicațiilor dintre card și cititorul de carduri.

O altă diferență este ușurința în utilizare, tehnologia NFC permite tranzacții mai rapide, deoarece nu necesită introducerea sau glisarea cardului, este suficient să ții cardul aproape de cititorul de carduri.

În ceea ce privește vulnerabilitatea, cardurile cu bandă magnetică sunt considerate mai vulnerabile la atacuri de fraudă și skimming, deoarece datele stocate pe banda magnetică sunt statice și pot fi ușor copiate sau ignorate de infractori. Cardurile NFC sunt considerate mai sigure, dar sunt în continuare vulnerabile la atacuri, cum ar fi atacurile prin skimming și releu, în care un infractor folosește un dispozitiv pentru a intercepta comunicarea dintre card și cititorul de carduri.

Banca online

Banca online este o metodă de plată electronică care permite clienților să acceseze informațiile contului lor bancar, să plătească facturile, să transfere fonduri și să vadă istoricul tranzacțiilor, totul printr-un computer sau un dispozitiv mobil conectat la internet. Multe bănci și instituții financiare oferă clienților lor servicii bancare online, care pot fi accesate printr-un site web sau o aplicație mobilă.

Pentru a utiliza serviciile bancare online, clienții trebuie mai întâi să își creeze un cont la banca sau instituția lor financiară. Odată configurat contul, clienții se pot conecta la contul lor prin intermediul site-ului web al băncii sau al aplicației mobile și să acceseze diverse funcții, cum ar fi soldurile contului, istoricul tranzacțiilor și posibilitatea de a transfera fonduri între conturi sau de a plăti facturile.

Unul dintre principalele beneficii ale serviciilor bancare online este confortul. Clienții își pot accesa informațiile contului și pot efectua plăți în orice moment, de oriunde, atâta timp cât au acces la internet. În plus, operațiunile bancare online le permit clienților să configureze plăți automate, cum ar fi pentru facturi și abonamente,

ceea ce poate economisi timp și poate reduce riscul de nerespectare a plăților.

Un alt avantaj al serviciilor bancare online este că îi poate ajuta pe clienți să-și țină evidența cheltuielilor, deoarece pot vizualiza istoricul tranzacțiilor și soldurile contului într-un singur loc. Serviciile bancare online le permit clienților să-și vadă informațiile contului și să efectueze plăți prin dispozitivele lor mobile, ceea ce permite accesul ușor la informațiile contului și posibilitatea de a efectua plăți în deplasare.

Banca online oferă, de asemenea, un nivel ridicat de securitate, deoarece toate tranzacțiile sunt criptate în timpul transmiterii pentru a preveni fraudă. Băncile au, de asemenea, măsuri de securitate pentru a proteja informațiile contului clientului, cum ar fi autentificarea cu mai mulți factori și alertele de securitate pentru activități suspecte.

Plăți mobile

Plățile mobile, cunoscute și ca bani mobili sau portofel mobil, permit clienților să efectueze plăți direct de pe smartphone-urile lor. Acest lucru se poate face prin tehnologia de comunicare în câmp (NFC), care permite plăți fără contact, sau prin aplicații mobile care se conectează la cardul de credit sau de debit al unui utilizator. Unii furnizori populari de plăți mobile includ Apple Pay, Google Wallet și Samsung Pay.

Pentru a utiliza plățile mobile, clienții trebuie mai întâi să configureze portofelul mobil pe smartphone-ul lor și să îl conecteze la un card de credit sau de debit. Odată configurat portofelul, clienții pot efectua plăți ținând telefonul aproape de un terminal de plată contactless sau folosind un cod QR. Unii furnizori de plăți mobile permit, de asemenea, clienților să efectueze plăți prin utilizarea unui cod de bare sau prin introducerea unui cod unic.

Plățile mobile permit clienților să efectueze plăți fără a fi nevoiți să transporte numerar sau carduri. În plus, plățile mobile folosesc adesea autentificarea biometrică, cum ar fi amprenta digitală sau recunoașterea facială, pentru a confirma identitatea utilizatorului înainte de a permite efectuarea unei plăți, ceea ce adaugă un nivel suplimentar de securitate.

Un alt avantaj al plăților mobile este că pot fi utilizate pentru achiziții online și achiziții în aplicație. Clienții pot face cu ușurință plăți pentru bunuri și servicii prin intermediul smartphone-urilor lor, fără a

fi nevoie de numerar sau carduri. Plățile mobile sunt utile și pentru clienții care sunt preocupați de securitatea transportului de carduri de credit sau de debit.

Plățile mobile sunt, de asemenea, deosebit de populare în țările în curs de dezvoltare, unde multe persoane nu au acces la serviciile bancare tradiționale. De asemenea, sunt utile pentru tranzacțiile transfrontaliere, deoarece permit clienților să efectueze plăți în diferite valute.

Carduri preplătite

Cardurile preplătite sunt o formă de plată electronică care poate fi utilizată în moduri similare cu cardurile de credit și de debit. Acestea sunt de obicei emise de instituții financiare, comercianți cu amănuntul sau procesatori de plăți. Utilizatorii încarcă fonduri pe card și le pot folosi pentru a face achiziții sau a retrage numerar. Cardurile preplătite sunt deosebit de utile pentru clienții care nu au un istoric de credit sau nu se pot califica pentru un card de credit sau pentru cei care doresc să-și controleze cheltuielile.

Pentru a utiliza un card preplătit, clienții trebuie mai întâi să achiziționeze cardul și apoi să încarce fonduri pe acesta. Acest lucru se poate face prin achiziționarea cardului de la un comerciant cu amănuntul, o instituție financiară sau online și apoi adăugarea de fonduri pe card prin depunerea de numerar, transferul de fonduri dintr-un cont bancar sau folosind un card de credit sau de debit. Odată ce cardul este încărcat cu fonduri, acesta poate fi folosit pentru a face achiziții oriunde sunt acceptate carduri de credit și de debit și poate fi folosit și pentru a retrage numerar de la bancomate.

Unul dintre principalele beneficii ale utilizării unui card preplătit este controlul pe care îl oferă asupra cheltuielilor. Deoarece cardul este încărcat cu o sumă stabilită de fonduri, acesta poate ajuta clienții să își bugeteze și să evite cheltuirea excesivă. În plus, cardurile preplătite au adesea caracteristici de securitate adăugate, cum ar fi numerele PIN, care pot ajuta la protejarea împotriva fraudei.

Portofele electronice

Portofelele electronice, cunoscute și sub denumirea de portofele digitale, sunt o formă de plată electronică care le permite clienților să stocheze și să gestioneze informațiile cardului de credit și de debit, precum și alte metode de plată, într-un singur loc.

Acestea permit clienților să efectueze plăți rapide și ușoare online sau în magazin, fără a fi nevoie să introducă de fiecare dată detaliile cardului.

Pentru a utiliza un portofel electronic, clienții trebuie mai întâi să creeze un cont și să-l conecteze la una sau mai multe metode de plată, cum ar fi carduri de credit sau de debit, conturi bancare sau carduri preplătite. Acest lucru se poate face printr-un site web sau o aplicație mobilă. Odată ce contul este configurat, clienții pot folosi portofelul electronic pentru a efectua plăți la comercianții care acceptă plăți prin portofel electronic. Acest lucru se poate face prin scanarea unui cod QR, introducerea unui cod unic sau atingând dispozitivul mobil pe un terminal fără contact. Furnizori populari de portofel electronic ar fi Apple Pay, Google Wallet, PayPal sau Venmo. Aceste portofele electronice au, de asemenea, funcții precum recompense, cashback și reduceri de care pot beneficia utilizatorii.

Unul dintre principalele avantaje ale utilizării portofelelor electronice este securitatea adăugată pe care o oferă, deoarece portofelele electronice folosesc adesea autentificarea biometrică, cum ar fi amprenta digitală sau recunoașterea facială, pentru a confirma identitatea utilizatorului înainte de a permite efectuarea unei plăți. În plus, portofelele electronice pot ajuta clienții să țină evidența cheltuielilor lor, deoarece pot vizualiza istoricul tranzacțiilor și soldurile contului într-un singur loc. De asemenea, pot fi folosite pentru a stoca informații despre cardul de fidelitate și cardurile de membru. Portofelele electronice sunt utile pentru achiziții online, deoarece permit clienților să efectueze plăți fără a fi nevoie să introducă detaliile cardului de fiecare dată când fac cumpărături. Acest lucru poate economisi timp și poate reduce riscul de erori sau fraudă. Portofelele electronice sunt utile și pentru clienții care preferă să nu poarte numerar sau carduri. De asemenea, sunt utile pentru tranzacțiile transfrontaliere, deoarece permit clienților să efectueze plăți în diferite valute.

Cecurile electronice

Cecurile electronice sunt o metodă de plată electronică care funcționează în mod similar cu cecurile tradiționale pe hârtie. Acestea sunt folosite pentru a efectua plăți dintr-un cont bancar în altul prin intermediul rețelei Automated Clearing House (ACH). Cecurile electronice sunt utilizate în mod obișnuit pentru plăți

recurente, cum ar fi facturile și abonamentele, și pentru companiile care doresc să proceseze plățile rapid și în siguranță. Pentru a utiliza un cec electronic, clienții trebuie mai întâi să furnizeze comerciantului informațiile contului lor bancar. Acest lucru se poate face de obicei printr-un formular online sau prin furnizarea unui cec anulat. Odată ce informațiile contului sunt introduse, clientul poate autoriza comerciantul să retragă fonduri din contul său în mod recurent sau pentru o anumită tranzacție. Procesul unei tranzacții cu cec electronic este similar cu cel al unui cec tradițional pe hârtie. Informațiile despre contul bancar al clientului sunt folosite pentru a crea o versiune electronică a cecului, care este apoi trimisă băncii comerciantului pentru procesare. Fondurile sunt apoi transferate din contul clientului în contul comerciantului. Unul dintre principalele avantaje ale utilizării cecurilor electronice este viteza cu care sunt transferate fondurile. Cecurile electronice sunt procesate electronic, ceea ce înseamnă că fondurile sunt transferate mult mai rapid decât în cazul cecurilor tradiționale pe hârtie. Cecurile electronice oferă, de asemenea, un nivel ridicat de securitate, deoarece informațiile contului sunt criptate în timpul transmiterii pentru a preveni fraudă. În plus, cecurile electronice pot ajuta clienții să țină evidența cheltuielilor lor, deoarece pot vizualiza istoricul tranzacțiilor și soldurile contului într-un singur loc. Un alt avantaj al cecurilor electronice este că pot fi folosite pentru plăți recurente, cum ar fi facturile și abonamentele, ceea ce poate economisi timp și poate reduce riscul de nerespectare a plăților. Cecurile electronice pot fi folosite și pentru companiile care doresc să proceseze plățile rapid și în siguranță. În general, cecurile electronice sunt o modalitate convenabilă și sigură de a efectua plăți electronice și devin din ce în ce mai populare atât pentru consumatori, cât și pentru companii.

Criptomonedele

Criptomonedă este o monedă digitală sau virtuală care utilizează criptografie pentru securitate și funcționează independent de o bancă centrală. Tranzacțiile cu criptomonedă sunt înregistrate pe un registru digital descentralizat numit blockchain. Bitcoin este cea mai cunoscută și folosită criptomonedă, dar există multe alte tipuri de criptomonedă, cum ar fi Ethereum, Litecoin și Ripple. Pentru a utiliza criptomonedă pentru plăți electronice, clienții trebuie mai întâi să achiziționeze criptomonedă printr-un proces numit mining sau achiziționând-o pe un schimb de criptomonedă. Odată ce clientul

are criptomoneda, o poate folosi pentru a efectua plăți către comercianții care o acceptă ca formă de plată. Procesul de plată implică, de obicei, clientul să trimită criptomoneda la adresa portofelului de criptomonede a comerciantului. Unul dintre principalele beneficii ale utilizării criptomonedei pentru plăți electronice este nivelul ridicat de securitate pe care îl oferă, deoarece toate tranzacțiile sunt înregistrate pe un registru descentralizat și sunt criptate în timpul transmiterii. Tranzacțiile cu criptomonede sunt, de asemenea, rapide și pot fi procesate 24/7, spre deosebire de sistemele bancare tradiționale care sunt închise în weekend și sărbători. În plus, tranzacțiile cu criptomonede sunt de obicei mai puțin costisitoare decât metodele tradiționale de plată electronică, deoarece nu implică comisioane pentru intermediari, cum ar fi băncile și procesatorii de plăți. Un alt avantaj al utilizării criptomonedei pentru plăți electronice este anonimatul pe care îl oferă, deoarece tranzacțiile cu criptomonede nu necesită partajarea informațiilor personale.

Ca o sumarizare, plățile electronice se pot realiza în amănunțite feluri, în funcție de disponibilitatea comerciantului și de posibilitățile sau necesitățile clientului, și anume:

- **Plăți cu cardul de credit:** cardurile de credit sunt o formă populară de plată electronică. Acestea permit clienților să facă achiziții și să le plătească mai târziu, de obicei cu dobândă. Plățile cu cardul de credit pot fi efectuate în persoană folosind un card fizic sau online, folosind informațiile cardului virtual.
- **Plăți cu cardul de debit:** cardurile de debit sunt conectate la contul bancar al unui client și permit efectuarea plăților electronice direct din acel cont. Ele pot fi folosite în persoană sau online și sunt adesea folosite pentru achiziții de zi cu zi, cum ar fi alimente sau benzină.
- **Transferuri electronice de fonduri (EFT):** EFT-urile sunt un tip de plată electronică care permit transferarea fondurilor direct dintr-un cont bancar în altul, fără a fi nevoie de numerar sau de un cec fizic. Acest tip de plată se poate face prin servicii bancare online, servicii bancare telefonice sau la un bancomat.
- **Plăți mobile:** plățile mobile se fac folosind un dispozitiv mobil, cum ar fi un smartphone. Acestea pot include portofele mobile, cum ar fi Apple Pay sau Google Wallet, care permit clienților să efectueze plăți ținând dispozitivul în apropierea

unui terminal de la punctul de vânzare. De asemenea, poate include plăți prin SMS și aplicații mobile.

- **Portofele digitale:** portofelele digitale sunt portofele virtuale care stochează informații de plată, cum ar fi numerele de card de credit, și permit efectuarea ușoară a achiziției pe site-uri web și aplicații. Acestea pot fi conectate la un card de credit sau de debit și permit clienților să efectueze plăți fără a fi necesar să introducă informațiile cardului lor de fiecare dată.
- **Plăți cu criptomonede:** plățile cu criptomonede se fac folosind monede digitale, cum ar fi Bitcoin. Aceste plăți se fac direct de la o persoană la alta, fără a fi nevoie de o bancă sau alt intermediar. Tranzacțiile sunt înregistrate pe un registru public descentralizat numit blockchain.
- **Plăți ACH:** plățile ACH sunt plăți electronice efectuate prin intermediul rețelei Casei de Compensare Automatizate. Aceste plăți sunt utilizate de obicei pentru depunerea directă a statelor de plată sau pentru plățile electronice ale facturilor. Sunt sigure, eficiente și rentabile.
- **Transfer bancar:** un transfer bancar este un transfer electronic de fonduri de la un cont bancar la altul, printr-o rețea precum SWIFT sau Fedwire. Transferul bancar este o modalitate rapidă de a muta bani între conturi bancare, dar poate fi mai costisitor decât alte metode de plată electronică și poate avea cerințe suplimentare de securitate.

Realizarea unei plăți electronice

O plată electronică este un tip de tranzacție financiară care este procesată prin rețele electronice, cum ar fi internetul, și nu necesită utilizarea de numerar fizic sau cec. Procesul unei plăți electronice implică de obicei următorii pași:

1. Clientul inițiază plata furnizând informațiile de plată, cum ar fi detaliile cardului de credit sau de debit, informații despre contul bancar sau informații despre portofelul electronic, comerciantului.
2. Comerciantul procesează plata trimițând informațiile de plată ale clientului procesatorului de plăți sau instituției financiare pentru verificare și autorizare.
3. Procesatorul de plăți sau instituția financiară verifică informațiile de plată ale clientului și autorizează tranzacția.

4. Odată ce tranzacția este autorizată, procesatorul de plăți sau instituția financiară trimite fondurile în contul comerciantului.
5. Comerciantul confirmă plata către client, iar tranzacția este finalizată.
6. Procesul de plată este înregistrat și stocat pentru referințe și urmărire viitoare.

O altă metodă utilizată în plățile electronice este tokenizarea, care este realizată prin înlocuirea datelor sensibile cu date care nu sunt sensibile. Este o metodă observată mai ales în procesarea datelor de card. Acest proces implică următorii pași:

1. Clientul înregistrează un card de credit pe telefonul mobil.
2. Cardul este înregistrat pe Server-ul de servicii de token.
3. Server-ul de servicii de token atribuie clientului un token temporar, care înlocuiește numărul de card real.
4. Când telefonul este utilizat pentru realizarea unei plăți cu ajutorul tehnologiei de câmp apropiat (NFC), acesta plătește cu ajutorul token-ului atribuit anterior.
5. Token-ul este trimis de către server-ul de procesare al plăților al vânzătorului către server-ul de servicii de token, pentru validarea cardului.
6. Server-ul de servicii de token compară token-ul trimis de vânzător cu token-ul înregistrat și validează plata.

Procesarea plăților se referă la seria de pași care au loc atunci când un client face o achiziție folosind un card de credit sau de debit. Procesul începe atunci când un client își prezintă cardul unui comerciant sau introduce online informațiile cardului. Informațiile de plată sunt apoi trimise unui procesator de plăți, care este o companie specializată în gestionarea și aprobarea sau respingerea tranzacțiilor.

Procesatorul de plăți verifică informațiile cardului cu emitentul cardului și verifică dacă clientul are fonduri suficiente pentru a finaliza tranzacția. În cazul în care tranzacția este aprobată, procesatorul de plăți trimite o autorizare comerciantului, care poate apoi onora comanda clientului. Procesatorul de plăți trimite apoi fondurile în contul bancar al comerciantului. Procesul include, de asemenea, diferitele măsuri de securitate, cum ar fi detectarea și prevenirea fraudei, tokenizarea și criptarea pentru a se asigura că informațiile sensibile ale clientului, cum ar fi numărul cardului de credit, data de expirare și CVV, sunt protejate împotriva accesului neautorizat.

Astfel, procesarea plăților este procesul de gestionare și aprobare sau refuzare a informațiilor de plată ale unui client, cum ar

fi cardul de credit sau de debit, pentru a finaliza o achiziție. Procesatorii de plăți sunt responsabili pentru verificarea informațiilor cardului, verificarea fondurilor suficiente și trimiterea unei autorizații comerciantului. Acestea includ, de asemenea, diverse măsuri de securitate pentru a proteja informațiile sensibile și pentru a preveni fraudă.

Măsuri de securitate

În timpul procesului, informațiile de plată și fondurile sunt transferate electronic, folosind rețele și protocoale securizate pentru a preveni fraudă și accesul neautorizat [6]. Unele dintre cele mai frecvent utilizate rețele și protocoale securizate în plățile electronice include numeroase metode de protejare a datelor sensibile, precum:

- **SSL/TLS:** Secure Sockets Layer (SSL) și Transport Layer Security (TLS) sunt protocoale de criptare care sunt utilizate pentru a securiza tranzacțiile online. Ele criptează datele transmise între dispozitivul clientului și serverul comerciantului, ceea ce face dificilă interceptarea sau accesarea informațiilor de către hackeri.
- **PCI DSS:** Standardul de securitate a datelor pentru industria cardurilor de plată (PCI DSS) este un set de standarde de securitate concepute pentru a proteja împotriva fraudei cu cardul de credit. Se aplică tuturor organizațiilor care acceptă, procesează, stochează sau transmit informații despre cardul de credit și le solicită să implementeze măsuri stricte de securitate pentru a proteja aceste informații sensibile.
- **EMV:** Europay, Mastercard și Visa (EMV) este un standard global pentru plățile cu cardul de credit și debit. Utilizează tehnologia cu cip pentru a oferi un plus de securitate, făcând mai dificil pentru fraudatori să copieze sau să ignore informațiile cardului [6].
- **Autentificare cu doi factori (2FA):** autentificarea cu doi factori este un nivel suplimentar de securitate care este utilizat pentru a confirma identitatea clientului. De obicei, implică o combinație de ceva ce știe clientul (de exemplu, o parolă) și ceva pe care îl are (de exemplu, un dispozitiv mobil sau un token de securitate) pentru a accesa contul.
- **Tokenizare:** Tokenizarea este un proces în care informațiile sensibile, cum ar fi numerele cardurilor de credit, sunt

înlocuite cu un simbol unic. Acest token poate fi apoi folosit pentru a finaliza o tranzacție fără a fi nevoie să transmită informațiile sensibile reale.

- Criptare: Criptarea este procesul de codificare a informațiilor astfel încât acestea să poată fi accesate numai de către părțile autorizate. Acest lucru ajută la protejarea informațiilor sensibile împotriva accesului neautorizat.
- Actualizări regulate de software și securitate: organizațiile trebuie să își actualizeze în mod regulat software-ul și sistemele de securitate pentru a se asigura că sunt protejate împotriva celor mai recente amenințări și vulnerabilități.
- Plan de răspuns la incident: organizațiile trebuie să aibă un plan de răspuns la incident pentru a gestiona încălcările de securitate și alte incidente de securitate, inclusiv încălcările datelor și atacurile cibernetice.
- Firewall: Firewall-urile sunt sisteme de securitate care sunt utilizate pentru a proteja o rețea de accesul neautorizat. Organizațiile trebuie să implementeze firewall-uri pentru a-și proteja rețelele de atacurile cibernetice.

Toate aceste rețele și protocoale securizate sunt folosite pentru a proteja informațiile sensibile și fondurile transferate. De asemenea, acestea sunt actualizate în mod regulat pentru a se adapta la noile forme de amenințări și atacuri asupra sistemelor electronice de plată.

Procesatoare de plăți online

În 2024 în România s-au făcut plăți online în valoare de 11.7 miliarde euro, cu 10% mai mult decât în 2023, reprezentând 3.4% din PIB-ul țării. Pentru aceste plăți se folosesc în prezent, în general, firme procesatoare de plăți care oferă servicii de plată prin plăți cu cardul, transfer bancar sau portofel electronic. Pe lângă tranzacția în sine, un procesator de plăți este util deoarece asigură securitatea tranzacțiilor prin sisteme avansate, protejând de fraudă părțile implicate. Conform BNR sau Visa, în 2023 peste 78% din români au efectuat cel puțin o plată online folosind în 75% din cazuri carduri bancare. Ca și variante de plată alternative sunt sisteme și aplicații de tip portofel digital cum ar fi Google Pay, Apple Pay sau Revolut, sau linkuri de plată. Se practică, pentru sume mai mari, și plata în rate fără dobândă.

În țara noastră, cele mai uzuale firme care se ocupă de procesarea plăților online sunt EuPlătesc, Klarna, Noda, Netopia sau MobilPay, Oney, PayPal, PayU, PlatiOnline, Revolut, Stripe sau VivaWallet.

Ca și posesor de business în mediul online, ar trebui avute în vedere câteva aspecte cum ar fi tipul de mărfuri sau servicii oferit spre vânzare și, în acord cu aceasta, tipul de clienți pe care îi ai și zona e prețuri. Pentru prețuri mici sau modice ale produselor, se potrivesc anumite politici, la prețuri mari este utilă și varianta de rate. De asemenea este de văzut dacă clienții sunt în țară sau în străinătate, dacă este nevoie să accepți mai multe tipuri de plăți sau de valute. Important este ca mereu, în afară de posibilitățile și beneficiile firmei, să se aibă în vedere și siguranța și preferințele clienților.

Pentru procesarea plăților este nevoie ca firma respectivă să aibă certificare PCI DSS, adică Payment Card Industry Data Security Standard, adică atestarea că această organizație respectă cerințele stricte de securitate în ce privește protecția datelor de card împotriva fraudelor și furturilor. Acest standard creat în septembrie 2006 este administrat de către consiliul de standarde de securitate PCI Security Standards Council (PCI SSC). Având această certificare, se confirmă că organizația îndeplinește cerințele din condițiile de standard. Se dorește preîntâmpinarea breșelor de securitate, fraudei sau a furtului de date.

Pentru dezvoltarea și menținerea siguranței datelor, a monitorizării și testării sistemelor în mod regulat, se instalează firewall-uri, software antivirus și criptarea datelor. Astfel se protejează transmisiile de date și accesul la acestea, aplicându-se totodată politici de securitate a informațiilor. De obicei aceste organizații sunt evaluate de către evaluatori de securitate QSA pentru obținerea certificării.

Companiile care se ocupă de gestionarea, stocarea sau transmiterea de date referitoare la carduri și posesorii acestora, trebuie să respecte PCI DSS. Comercianții cu amănuntul, procesatorii de plăți, băncile, dezvoltatorii de software, producătorii de hardware, companiile de hosting, uniuni de credit, companiile de telefoane, toți trebuie să respecte aceste standarde.

Standardul PCI DSS conține un set de reguli pentru asigurarea securității informațiilor conținute în aceste tranzacții și transmisii de date. Ca tipuri de activități incluse în aceste reguli sunt:

- Construirea și menținerea unor rețele securizate;

- Protejarea datelor titularilor de carduri;
- Utilizarea unei criptografii puternice;
- Controlarea accesului la datele titularilor de card;
- Monitorizarea și testarea rețelilor;
- Implementarea unor politici de securitate a informațiilor.

Implementarea conformă și respectarea acestor reguli, configurarea corespunzătoare a măsurilor de securitate prevăzute, pot reprezenta pentru firme o adevărată provocare. Ca și cauze pot fi lipsa de resurse, insuficienta experiență sau definirea și clasificarea imprecisă a mediului de date.

Prezentăm în continuare diferite metode de plată care există în prezent în lume, vorbind astfel de metode tradiționale, internaționale și locale.

Metode de plată internaționale – Exemple			
Plăți cu cardul:	Portofel digital:	Plăți instantanee:	Transfer bancar:
American Express	Alipay (China)	CIMB Clicks (Asia)	AmBank (Malaezia)
Carte Bleue	ApplePay	Eps (Austria)	Danske (Nordic)
Diners	DragonPay (Filipine)	Finnish Banks (Finlanda)	HongLeong (Malaezia)
Discover	Mach	IDEAL (Olanda)	Maybank2U (Malaezia)
JCB	MercadoPago (America Latină)	Multibanco-	Wire Transfer
Maestro	MrCash (Belgia)	SIBS (Portugalia)	
MasterCard	PayPal (200 de țări)	Nordea (Europa de Nord)	
UnionPay	Solo (SriLanka)	OP-Pohjola (Finlanda)	
Visa	ToditoCash (Mexic)	PagoEfectivo (Peru)	

	WebMoney	Pix (Brazilia)	
	WeChatPay (China)	Przelewy24 (Polonia)	
	GooglePay	Sofort (Germania)	
	ToditoCash (Mexic)	Trustly (Europa)	
		Boleto (OXXO PayPro Global)	
		OXXO (Mexic)	

Vulnerabilități în comerțul electronic

Când a fost creat de către Tim Berners Lee și apoi asociații, internetul a fost considerat și oferit spre utilizare ca un mediu de încredere și acces deplin, respect reciproc al utilizatorilor. Se considera ca o protecție minimă era suficientă. În timp însă, o data cu extinderea accesului la internet, utilizatorii au devenit de o diversitate tot mai mare, astfel încât în timp, au apărut diverse pericole. Dintre primele pericole istorice amintim:

- Viermele internet din 1988, afectând câteva mii de computere
- Incidentul Berferd în 1991
- Furtul de parole ale furnizorilor de servicii de internet din anii 93-94
- Interceptarea unor pachete IP de la centrul din San Diego din 1994
- Furturi de fonduri la Citybank în 1995

De fapt, atacurile reușesc în urma unor erori în scrierea programelor, neglijență de administrare sau a utilizatorilor, lipsa parțială sau totală de securizare a protocoalelor TCP/IP.

Pe tema istoricului dezvoltării tehnologice a internetului în paralel cu dezvoltarea tipurilor de atacuri online în relație cu magazinele digitale, se pot lansa teme de cercetare, de comparație (avantaje - dezavantaje) în raport cu magazinele clasice. Se pot realiza dezbateri referitoare la diferitele situații de pericole întâlnite personal de fiecare dintre participanți precum și modurile de soluționare a situațiilor de criză.

Sunt prezentate în continuare diferite tipuri de posibile atacuri, împreună cu sugestii pentru ajutarea la evitarea acestora.

Pe lângă succinta explicare a termenilor de bază într-un dicționar, se dorește discutarea fiecărui paragraf în parte, legat de experiența studenților pe diferitele situații.

Social engineering = Acesta este un alt mod de amenințare care poate apărea în mediul online și reprezintă arta de a manipula, minți, sau influența pe ceilalți ca să execute anumite acțiuni ori să divulge informații confidențiale. Este un mod de a câștiga încrederea, termenul aplicându-se celor care folosesc tertipuri pentru a culege informații sau pentru a accesa sistemele informatice, de cele mai multe ori atacatorul nu ajunge față-în-față cu victima. La acest capitol putem avea:

PHISHING sau SMS-ishing = formă de activitate criminală care constă în obținerea datelor confidențiale, cum ar fi credențialele de acces de tip username, parola, PIN pentru aplicații financiare sau alte informații referitoare la cardul de credit, prin tehnici de manipulare a identității unei persoane sau a unei instituții. Un atac de tip phishing constă, în mod normal, în trimiterea de către atacator a unui mesaj electronic, folosind programe de e-mail sau telefon în care utilizatorul este sfătuit să introducă credențialele de access (nume utilizator, parola), numere de card, coduri PIN, etc.

Exemplu de phishing: primiți un email în care ați fost informat că ați câștigat o excursie în străinătate iar tot ce trebuie să faceți pentru a primi voucherul de călătorie este să introduceți pe un site asemănător cu cel al băncii, pentru a confirma identitatea: numele, adresa și datele cardului.

Exemplu de sms-ishing: primiți un mesaj SMS de la un număr necunoscut care pretinde a fi banca dvs. și care va invită să descărcați o nouă versiune a aplicației de mobile banking. Cel mai probabil în acest caz veți descărca și rula un malware care va da atacatorului posibilitatea să controleze și să monitorizeze telefonul mobil, inclusiv să poată captura credențialele de acces pentru aplicația legitimă de online banking.

V-ISHING = voice + phishing, o formă de înșelătorie prin care utilizatorul este păcălit să furnizeze informații sensibile, credențialele de acces, numere de card, sau coduri de acces, cu scopul de a

impersona utilizatorul de drept sau a fi folosite de atacator în alte atacuri de inginerie socială.

Exemplu de v-ishing: primiți un telefon de la o persoană care pretinde a fi un angajat al băncii care dorește să verifice numărul cardului, codul PIN sau codul de securitate al cardului deoarece a fost inițiată o alertă de securitate.

De cele mai multe ori adresa de mail sau numărul de telefon sunt culese din surse publice cum ar fi site-uri de anunțuri sau din baze de date făcute publice prin breșe de securitate, unde pentru servicii online s-au furnizat date de contact. Atacatorii nu știu fiecare persoană cu ce bancă sau bănci lucrează, dar mizează pe faptul că nimeresc la un moment dat. Dacă primiți un mail sau sms suspect, cel mai bine este să ștergeți mesajul, mai ales dacă te provoacă să apeși pe un link sau să deschizi vreun atașament. De asemenea, dacă aveți suspiciuni cu privire la originea unui mesaj de tip email sau sms, este bine să contactați banca pe unul din canale de suport oficiale cum ar fi telefonul sau email-ul menționat pe websiteul public.

CEO FRAUD = sau Business Email Compromise(BEC), se referă la situația în care atacatorul reușește să compromită serverul de email al unei companii sau să creeze o căsuță de email asemănătoare cu cea oficială a companiei vizate, de exemplu schimbând o literă, cifra zero (0) în loc litera O. Atacatorul folosește această identitate falsă pentru a informa prin email partenerii de afaceri ai companiei cu privire la schimbarea conturilor de plată a facturilor. De obicei persoana care este impersonată este directorul companiei sau directorul financiar. În email-ul trimis, directorul financiar precizează că începând de acum înainte plățile către companie să fie efectuate într-un cont nou, cont care este de fapt la dispoziția atacatorului. Dacă partenerul de afaceri nu face verificări suplimentare și efectuează plata în contul indicat, banii ajung în posesia atacatorului.

Recomandări pentru evitarea unor asemenea situații:

- evitați să folosiți corespondența electronică neprotejată pentru vehicularea informațiilor cu caracter comercial sensibil sau cu caracter confidențial cum ar fi coduri IBAN, parole sau detalii de plată
- folosiți softuri antivirus pentru protecția calculatoarelor dvs
- nu efectuați plăți către conturi noi pe baza unor instrucțiuni primite prin email și fără să verificați mai întâi validitatea acestor conturi cu partenerii dvs, prin intermediul altor canale de comunicație care nu au legătură cu poșta electronică. Pe lipsa acestei verificări mizează infractorii, deci dacă o veți face, veți contracara cu succes tentativa

de fraudă. Verificarea nu o faceți în niciun caz prin e-mail sau prin mijloace de contact sugerate prin intermediul poștei electronice ci prin mijloace sigure și cunoscute, numere de telefon sau fax pe care le-ați mai folosit în trecut

- dacă ați efectuat o plată către un cont eronat, contactați urgent banca dvs. pentru a putea afla dacă mai sunt posibile demersuri de blocare/returnare a sumelor implicate.

De asemenea, în situația în care ați fost victima unei astfel de tentative de fraudă să înștiințați cât mai rapid organele de poliție locale.

Vânzarea online

Dacă persoanele doresc să vândă anumite bunuri sau produse apelează la diferite platforme on-line aparținând unor companii care se ocupă cu intermedierea pe internet ca pagini de vânzări-cumpărări online, în urma unei tranzacții încheiate pe o astfel de platformă vânzătorul primește un mesaj e-mail de la cumpărător. În acest mesaj cumpărătorul îi cere vânzătorului să expedieze obiectul vândut prin poștă, de obicei către destinații din zona continentului african (dar nu numai). Pentru a determina vânzătorul să expedieze produsul înaintea primirii prețului de achiziționare potențialul cumpărător include în mesajul e-mail o confirmare de plată (falsă). Din aceasta reiese, în mod eronat, faptul că s-a efectuat plata prin transfer bancar și că vânzătorul poate să intre în posesia banilor doar după ce va face dovada faptului că a expediat produsul către adresa indicată de falsul cumpărător. În realitate vânzătorul a fost înșelat și nici o sumă de bani nu a fost transferată de cumpărător. Astfel de mesaje frauduloase de confirmare a tranzacțiilor pot include logo-ul sau denumirea unor bănci cunoscute sau chiar numele unor angajați ai băncilor respective.

Pentru a preveni astfel de situații, este bine să:

- efectuați tranzacții pe platformele cunoscute de intermediari online
- verificați cu atenție reputația cumpărătorului și ce tranzacții a efectuat în trecut
- comunicați cu partenerul de afaceri și pe alte canale nu doar pe email
- verificați cu atenție termenii și condițiile platformei care intermediază vânzarea

Protecția terminalelor tehnologice

Terminale de comunicații pot fi calculatoare, laptopuri, tablete, telefoane mobile. Atactorii ținesc aceste terminale în speranța că ele nu sunt suficient protejate, iar prin compromiterea lor reușesc să desfășoare tranzacții frauduloase și să obțină câștiguri materiale.

Protecția calculatorului sau a laptopului

Instalați pe calculator sau laptop numai aplicații cu licență validă (comercială sau gratuită) și care provin din surse sigure (de ex: site-ul web al producătorului, CD/DVD-uri achiziționate împreună cu calculatorul/laptop-ul). De cele mai multe ori un software piratat descărcat dintr-o sursă care nu este de încredere ascunde și un malware!

Utilizați calculatoare sau laptopuri și sisteme de operare cu ultimele versiuni de Windows sau Linux, deoarece sistemele de operare moderne au controale de securitate îmbunătățite sau complet noi, iar acestea sunt activate implicit. Multe dintre aceste controale de securitate pot preveni sau limita impactul pentru multe dintre atacurile informatice. Aici sunt vizate de exemplu pachetele de aplicații de tip Microsoft Office, navigatoarele web cum ar fi Internet Explorer, Safari, Google Chrome, soluții de securitate - antivirus, antimalware, etc.

Instalați o soluție de securitate ce oferă cel puțin protecție anti-virus, anti-malware și anti-phishing sau soluții complexe care asigură și funcționalități de tip firewall și IPS (Intrusion Prevention System) de prevenire a atacurilor informatice precum și de navigare web securizată. Este important ca soluția de securitate să fie actualizată periodic cu ultimele semnături anti-virus.

Nu conectați dispozitive necunoscute la calculatorul cum ar fi stick-uri USB găsite în locuri publice care pot fi lăsate sau "uite" la îndemâna/la vedere intenționat de atacatori. Acestea pot conține viruși (sau alte tipuri de cod malițios), iar când sunt conectate la calculatorul dumneavoastră pot infecta în mod automat aceste dispozitive.

Efectuați copii de siguranță pentru datele dvs. pe un suport extern în mod periodic. Astfel vă puteți recupera fișierele în urma unei probleme hardware sau dacă ați fost victima unui atac de tip "ransomware", care vă restricționează accesul la fișiere prin criptarea

acestora. Suportul extern folosit pentru salvarea datelor să nu fie în permanență conectat la calculator ci doar atunci când efectuați copiile de siguranță.

Protecție pentru smartphone sau tableta

Protejați accesul la smartphone-ul sau tableta dumneavoastră folosind PIN, parola, sau "semn grafic". Atunci când este posibil actualizați sistemul de operare de pe smartphone-ul sau tableta dumneavoastră Android, iOS, Windows. Instalați aplicații doar din magazinele de aplicații oficiale ca Google Play, Apple App Store, Microsoft Store. Aplicațiile care provin din "magazine" necunoscute pot conține și cod malițios care vă poate infecta și compromite securitatea echipamentului.

Exemplu: împreună cu aplicația descărcată instalați și un malware de tip tojan care poate fura credențialele aplicației de mobile banking, precum și codurile OTP (One Time Passcode) primite prin SMS necesare pentru autorizarea plăților 3D Secure.

Pentru a evita pe cât posibil infectarea cu malware se recomandă să vă protejați telefonul sau tableta cu o aplicație antivirus. Este recomandat de asemenea să verificați și "permisiunile" pe care aplicațiile le solicită la instalare.

Dezactivați opțiunile de conectivitate (Wi-Fi, Bluetooth, NFC, etc) pe care nu le utilizați în mod curent. Eliminați astfel posibilele canale de intruziune pe care un potențial atacator le-ar putea utiliza, în plus, economisiți resursele bateriei și prelunghiți durata de funcționare a echipamentului.

Recomandări pentru plata pe internet

Nu este recomandat să accesați site-ul de Internet Banking al băncii dintr-un link primit pe email sau SMS. Navigați pe siteul oficial și folosiți linkurile de acolo. Linkurile primite pe email vă pot redirectiona către un site fals controlat de atacator. Acesta vă poate păcăli să introduceți credențialele de acces pe acest site fals controlat de atacatori. Nu dați click pe "Agree" sau "OK" pentru a închide o fereastră. În schimb, faceți click pe "X" în colțul ferestrei sau apăsați Alt+F4 pe tastatură.

Verificați cu atenție dacă atunci când desfășurați operațiuni financiare transferuri sau plăți cu cardul, conexiunea utilizată este una securizată (https://). Băncile folosesc certificate de securitate cu

validare extinsă și adresa siteului vizitat apare cu verde și poate fi văzută imaginea unui lăcățel închis în bară de adresa URL. Dacă browserul vă avertizează că există o problemă cu certificatul siteului este recomandabil să nu continuați și să contactați banca.

Salvarea automată a parolelor în browser nu reprezintă o opțiune pentru păstrarea în siguranță a acestora. Dacă doriți să păstrați securizat aceste date folosiți întotdeauna un manager de parole cum ar fi KeePass, 1Password, LastPass, RoboForm. Credențialele de acces (utilizator, parola, cod acces, etc) sunt informații personale și nu trebuie comunicate altor persoane. Nu notați pe foi hârtie sau în fișiere text nesecurizate aceste informații sensibile.

Urmăriți să folosiți parole complexe de minim 8 caractere, care să conțină cel puțin 4 caractere de forma o literă mare (A... Z), o literă mică (a... z), o cifră (0... 9) și un semn special cum ar fi !, @, #, \$, %, ?, ^, etc.

Pentru că există posibilitatea că parola dvs. să fie aflată odată cu trecerea timpului este recomandat că parola să fie schimbată periodic. De asemenea este foarte important să **NU FOLOSIȚI ACEEAȘI PAROLĂ** pentru mai multe servicii (ex. cont email, cont internet banking, cont rețea socializare, etc). Dacă aveți cel mai mic dubiu că o parolă a fost aflată (compromisă) schimbați-o imediat!

Aveți grijă ca nimeni să nu vă privească atunci când introduceți o parolă sau un cod PIN. Evitați să introduceți parole pe terminale (computere din internet cafe-uri, tablete, telefoane pe care nu le dețineți sau cunoașteți, aceste terminale pot avea instalate programe de tip keylogger care vă pot prelua credențialele de acces. Alegeți opțiunea de deconectare (Log Off sau Sign Out) atunci când nu mai folosiți un anumit serviciu.

Banciile nu apelează clienții săi pentru a cere informații precum: CNP, număr card, PIN, ID logare, parola, cod token sau orice alte informații personale. O astfel de cerere reprezintă o posibilă tentativă de fraudă și pentru siguranța dvs. este recomandat să informați banca folosind canalele oficiale.

Plățile cu cardul

Păstrați cardul bancar cu aceeași grijă cu care păstrați și actul de identitate. Memorați numărul Personal de Identificare (PIN), nu îl scrieți. Nu păstrați acest număr alături de card, scris în telefon sau altundeva unde poate fi citit de o altă persoană.

Dacă alegeți să păstrați documentul de la bancă, prin care vi s-a comunicat PIN-ul, în nici o situație să nu păstrați acest document în același loc unde este cardul, totuși nu se recomandă păstrarea documentului.

În cazul în care alegeți să vă creați un nou PIN sau să îl schimbați pe cel ce v-a fost dat, evitați alegerile evidente cum ar fi data nașterii personală sau a membrilor familiei.

Se recomandă să utilizați un PIN diferit pentru fiecare card pe care îl dețineți. Se recomandă de asemenea să semnați imediat pe banda de semnătură de pe spatele cardului, după ce îl primiți de la bancă. Se recomandă să păstrați securizat o listă cu numerele cardurilor pe care le dețineți, împreună cu numerele de contact unde trebuie să anunțați în cazul în care acestea au fost pierdute sau furate.

La efectuarea unei tranzacții pe internet sunt necesare:

Tipul cardului - Visa, MasterCard

Nume (așa cum apare pe card)

Numărul cardului (cele 4 grupuri a câte 4 cifre aflate pe card)

Data expirării cardului (se găsește sub numărul cardului și este de forma ll/aa)

CVV2 (Card Verification Value – nume utilizat de Visa) sau CVC2 (Card Verification Code – nume utilizat de MasterCard), acesta este un cod de siguranță format din 3 cifre și este tipărit pe verso-ul cardului. Mai poate fi întâlnit pe Internet și sub denumiri cum ar fi Card Security Code/Verification Code, parola sau codul OTP pentru tranzacții prin sistemul "3D Secure" (Verified by Visa, sau Mastercard Securecode), în cazul în care cardul este înrolat într-un astfel de sistem.

Toate aceste informații, mai puțin parola 3D Secure, se află înscrise pe card, de aceea trebuie să păstrați cardul în siguranță și să nu dați ocazia să fie obținute aceste informații de către alte persoane.

Parola 3D-Secure sau codul unic OTP sunt elemente de siguranță, de antifrauda, dezvoltate de VISA și MasterCard. Avantajele 3D Secure sunt:

Reducerea riscului de fraudă deoarece doar persoana care cunoaște parola 3D Secure, sau care cunoaște codul OTP creat unic pentru acea tranzacție 3D Secure și primit prin SMS, token sau alte canale, poate tranzacționa online pe site-uri care folosesc acest sistem antifraudă;

Dacă datele cardului dumneavoastră înrolat în 3D Secure sunt folosite fraudulos de către o terță parte pentru a comanda pe site-ul

unui comerciant care nu folosește acest sistem de protecție, veți avea câștig de cauză la disputarea sumei aferente tranzacției.

Nu răspundeți e-mailurilor care par a fi trimise de banca emitentă, în care vă sunt solicitate datele sensibile ale cardului număr card, data expirării, codul CVV2/CVC2, parola 3D Secure sau codul PIN, sub pretextul unor verificări, modificări, premii, culegerii de informații pentru respectarea unor modificări legislative etc.

Atunci când efectuați cumpărături online încercați să achiziționați de la comercianți cunoscuți, care se bucura de o bună reputație. Se recomandă folosirea pentru plățile pe Internet a unui card dedicat, acest card se poate atașa unui cont în care să aveți doar sumele pe care doriți să le utilizați în acest scop. Evitați folosirea cardurilor atașate conturilor de salarii sau cele cu descoperire de cont (overdraft).

Rețelele wireless (WiFi)

Evitați conectarea laptopului sau a smartphone-ului la o rețea wireless nesecurizată. Rețele Wi-Fi gratuite (restaurant, cafenele, aeroporturi) sunt cele mai vulnerabile dacă nu sunt securizate. Atunci când vă conectați la o rețea nesecurizată orice persoană aflată în raza de acțiune a rețelei ar putea intercepta traficul dvs. și “vedea” anumite informații ce au fost transmise nesecurizat. Dacă totuși sunteți nevoit să vă conectați la o astfel de rețea evitați să introduceți parole de acces sau să folosiți servicii financiare online.

Nu lăsați router-ul de acasă nesecurizat și nu folosiți protocolul de securizare WEP. Acest protocol nu este sigur și un atacator poate obține accesul la rețeaua wireless și intercepta traficul din această rețea. Se recomandă să folosiți protocolul WPA2, să configurați o parolă cât mai lungă și să schimbați numele implicit (SSID-ul) al rețelei wireless.

Schimbați parola preconfigurată din fabrică pentru interfața de administrare și configurare a router-ului, folosind o altă parolă puternică, deoarece parolele inițiale se pot găsi ușor pe internet și pot fi folosite de persoane rău voitoare care au acces în rețeaua dumneavoastră pentru a modifica în mod malițios anumite setări precum DNSul (putând fi astfel amenințați de un atac de tip “DNS Pharming”, unde chiar dacă introduceți manual și corect adresa web a băncii tale sau a instituției financiare direct în browser, vei deschide de fapt un site malițios de tip clonă, acest tip de atac fiind mult mai

periculos chiar decât atacul de tip Phishing pentru că nu exista modalități de identificare a site-ului malițios.

Social media

Evitați publicarea online a informațiilor personale, financiare, cum ar fi serie card, data expirare card, CVV, credentiale de acces la soluțiile internet banking, informații de localizare, pe siteurile social media ca Facebook, Twitter, Instagram, etc.

Folosiți opțiunile de protejare a intimității specifice fiecărui site și limitați expunerea informațiilor personale în mediul online. Fiți atenți la orice informație publicată pe site-urile de socializare. Aceste informații pot fi utilizate de atacatori, de exemplu sunt cazuri cunoscute de locuințe sparte de infractori, pentru că proprietarii publicaseră pe site-urile de socializare poze, comentarii, localizări din concedii, practic informând că nu sunt acasă pentru o perioadă de timp.

Fiți atenți la persoanele pe care le contactați în mediul online. Oricine își poate crea un cont pe site-urile de socializare asumându-și o altă identitate. Fiți suspicios atunci când sunteți contactat de prieteni sau cunoscuți în mediul online dacă comportamentul acestora este neobișnuit. De exemplu: primiți mesaje care conțin doar un link URL, sau email cu link URL sau fișiere atașate, dar fără nici o altă explicație sau într-un limbaj neobișnuit pentru prietenii dumneavoastră. Este posibil ca respectiva persoană să aibă contul compromis, iar atacatorul încearcă să intre în contact cu dumneavoastră, de exemplu pentru a vă infecta calculatorul. Evitați să urmați link-uri, fără o verificare prealabilă. Puteți fi redirectat spre un site compromis care găzduiește aplicații malware.

Vulnerabilități ale site-urilor la atacuri cibernetice și unele sugestii pentru evitarea acestor atacuri

În lumea tehnologiei existentă în prezent, accesul la Internet este o necesitate, fiind utilizat pentru obținere de informații, comunicare și multe altele. Cu toate acestea, odată cu creșterea activității cibernetice, cresc și amenințările atacurilor cibernetice. Mulți utilizatori nu înțeleg aceste amenințări sau cum să își protejeze datele personale în timp ce sunt conectați la Internet. Așadar, este vital ca utilizatorii să fie instruiți în vederea securității cibernetice.

Aplicațiile web sunt supuse amenințărilor, deoarece tind să fie vulnerabile. Penetration testing-ul (cunoscut și sub numele de Pentesting) este un proces structurat, efectuat pentru a evalua securitatea unei infrastructuri IT. Acest tip de testare se efectuează în mod regulat pentru a identifica riscurile și a le gestiona pentru a atinge standarde de securitate mai ridicate.

Pentru executarea Pentestingului, se utilizează aplicații vulnerabile disponibile public, scopul principal fiind acela de a-i face pe viitorii pasionați să învețe despre întregul proces pentru a securiza informațiile și nu a-i face capabili să atace aplicațiile web. Printre aplicațiile web care se utilizează în aceste scopuri se găsesc: Damn Vulnerable Web Application (DVWA), Mutillidae, TWiki.

OWASP Mutillidae II este o aplicație web gratuită, de tip open source, vulnerabilă în mod deliberat, reprezentând o țintă pentru pasionații de securitate web. Aceasta poate fi instalată pe sisteme de operare precum Linux și Windows, folosind LAMP, WAMP și XAMPP. Este preinstalată pe SamuraiWTF și OWASP BWA, iar versiunea existentă poate fi actualizată pe aceste platforme. Cu zeci de indicii pentru a ajuta utilizatorul, acesta este un mediu de hacking web ușor de utilizat, conceput pentru instrumente de evaluare a vulnerabilităților.

Open Web Application Security Project

Open Web Application Security Project (OWASP) prezintă problemele legate de securitatea aplicațiilor web, concentrându-se pe cele mai importante 10 vulnerabilități. Se recomandă tuturor companiilor să includă raportul OWASP în procesele lor, pentru a reduce riscurile de securitate. Modelul din 2017 OWASP Top 10 conține vulnerabilități la următoarele atacuri:

1. Injection – SQL, HTML injections
2. Broken authentication – Brute Force, Dictionary, Automated attacks
3. Sensitive data exposure – Compromising data
4. XML External Entities (XXE) – Attack on weakly configured XML parser
5. Broken access control – Exploiting authorization flaws
6. Security misconfigurations – Exploiting default settings
7. Cross Site Scripting (XSS) – Injecting client-side malicious code

8. Insecure deserialization – Insecure conversion of byte-strings to objects
9. Using components with known vulnerabilities – Exploiting outdated software
10. Insufficient logging and monitoring

Tipuri de atacuri cibernetice din top 10 OWASP

SQL Injection

- este una dintre cele mai comune amenințări la adresa unui sistem de baze de date, în care atacatorul introduce instrucțiuni SQL într-o casetă text, pentru a obține acces la resurse sau pentru a face modificări la datele stocate în baza de date. Lipsa validării intrărilor în aplicații face ca atacatorul să aibă succes. Un atac de tip SQL Injection poate dăuna bazei de date în diferite moduri, cum ar fi manipularea neautorizată a bazei de date sau recuperarea datelor sensibile. Poate fi folosit și pentru a executa comenzi la nivel de sistem care pot determina sistemul să refuze serviciul aplicației. Această problemă este foarte riscantă, deoarece poate cauza pierderea sau utilizarea greșită a datelor de către părți care nu sunt autorizate și, ca urmare, funcționalitatea și confidențialitatea sunt distruse.

Este important de reținut faptul că există metode pentru reducerea riscului de modificare/pierdere a datelor din cauza atacului SQL Injection. Cea mai bună metodă este să se utilizeze mai multe strategii, printre care regăsim:

- **Use of Prepared Statements (with Parameterized Queries):** Această metodă de „curățare” a intrărilor bazei de date solicită dezvoltatorilor să definească mai întâi tot codul SQL, iar apoi să transmită doar parametri specifici interogării SQL; datele introduse primesc în mod explicit un domeniu de aplicare limitat. Acest lucru permite bazei de date să facă distincția între datele care sunt introduse și codul care urmează să fie rulat, indiferent de tipul de date furnizate în câmpul de intrare.
- **Escape All User Supplied Input:** La scrierea codului SQL, anumite caractere sau cuvinte au o semnificație specială, cum ar fi caracterul „*”, care înseamnă „oricare” sau cuvântul „SAU”, care este condițional. Pentru a evita utilizatorii care

introduc aceste caractere, fie accidental, fie rău intenționat, într-o solicitare API către baza de date, intrarea furnizată de utilizator poate fi validată. Metoda de escape a unui caracter este modalitatea de a spune bazei de date să nu o analizeze ca o comandă sau condițional, ci să o trateze ca intrare literală.

- **Use of Stored Procedures:** Deși nu este o strategie de securitate robustă în sine, procedurile stocate pot ajuta la limitarea riscului asociat cu SQL Injection. Prin limitarea corectă a permisiunilor contului bazei de date care rulează interogări SQL, chiar și codul aplicației non-robuste care este vulnerabil la SQL Injection, atacatorul nu va avea permisiunile necesare pentru a manipula tabelele de baze de date.
- **Enforce Least Privilege:** În toate cazurile în care un site web trebuie să utilizeze SQL dinamic, este important să se reducă expunerea la SQL Injection prin limitarea permisiunilor la cel mai restrâns domeniu necesar pentru a executa interogarea relevantă. Aceasta înseamnă că un cont administrativ nu ar trebui să execute în niciun caz comenzi SQL ca urmare a unui apel API de la o solicitare neautorizată. În timp ce procedurile stocate sunt utilizate pentru interogările statice, aplicarea celui mai mic privilegiu poate ajuta la reducerea riscurilor interogărilor SQL dinamice.

HTML Injection

- Hypertext Markup Language (HTML) Injection este un atac asupra unui utilizator, făcut posibil printr-o vulnerabilitate de injectare într-o aplicație web.

Când o aplicație nu gestionează corect datele furnizate de utilizator, un atacator poate furniza HTML valid, de obicei printr-o valoare a unui parametru, și poate injecta propriul conținut în pagină. Acest atac este de obicei folosit împreună cu o anumită formă de inginerie socială, deoarece atacul exploatează o vulnerabilitate bazată pe cod și încrederea unui utilizator.

Este important ca posesorii site-urilor web să cunoască pericolele la care sunt expuși și efectele pe care le poate avea un posibil atac. Printre efectele atacului de tip HTML Injection asupra unui site web se numără următoarele:

- întârzierea serviciilor site-ului;
- atac de tip phishing pentru a amenința victima;
- înșelătorii la scară largă pentru amenințarea utilizatorilor de pe site-ul respectiv;
- modificarea site-ului web.

Există modalități de protejare a site-ului de un posibil atac și se recomandă a fi aplicate de toată lumea. O parte dintre acestea sunt următoarele:

- dezvoltatorul web ar trebui să aplice limita de cuvinte în fiecare câmp;
- dezvoltatorul web ar trebui să aplice firewall-ul pe fiecare câmp, astfel încât atacatorul să nu poată introduce etichetele care sunt elementele de bază ale codării html.

Brute Force Attack

- Acest tip de atac folosește o metodă de tip trial-and-error pentru a ghici informațiile de conectare, cheile de criptare sau pentru a găsi o pagină web ascunsă. Aceste atacuri sunt făcute prin „forță brută”, ceea ce înseamnă că hackerii folosesc încercări excesive pentru a încerca să „forțeze” intrarea în conturile private ale victimelor. De obicei, motivul din spatele lansării unui astfel de atac este utilizarea contului încălcat pentru a executa un atac la scară largă, a fura date sensibile, a închide sistemul sau o combinație a celor trei. Crearea unui cod care execută acest tip de atac nu necesită multă imaginație sau cunoștințe și există chiar și instrumente automate care trimit câteva mii de încercări de parole pe secundă.

Hackerii utilizează acest tip de atac, întrucât pot obține o serie de beneficia, precum următoarele:

- profitul din reclame sau colectarea de date despre activitate;
- furtul de date personale și obiecte de valoare;
- răspândirea programelor malware pentru a provoca întreruperi;
- deturnarea sistemului pentru activitate rău intenționată;

Pentru a preveni posibilitatea confruntării cu un astfel de atac, în primul rând este important ca parolele fiecărui cont al utilizatorilor de aplicații să fie cât mai complexe. De asemenea, printre metodele de prevenire se mai găsesc:

- limitarea încercărilor eșuate de conectare;
- oprirea accesului utilizatorului root prin SSH prin editarea fișierului `sshd_config`;
- evitarea utilizării un port implicit, editarea liniei portului în fișierul `dvs.sshd_config`;
- folosirea Captcha;
- limitarea conectărilor la o adresă sau un interval de adrese IP specificat;
- autentificare cu doi factori;
- adrese URL de conectare unice;
- monitorizarea jurnalelor serverului.

Sensitive data exposure

- Atacurile de acest tip au loc atunci când o aplicație expune accidental date sensibile. Acestea diferă de data breaches, în care un atacator accesează și fură informații. Sensitive data exposure apare de obicei atunci când nu se reușește protejarea în mod adecvat a informațiilor din baza de date. Dintre cauzele care pot permite expunerea la un astfel de atac pot fi criptarea slabă sau inexistentă, erori de software sau stocarea datelor în locuri greșite.

Un atacator poate expune diferite tipuri de date. Dintre acestea fac parte: detaliile contului bancar, datele cardului de credit, datele privind asistența medicală, session tokens, numerele de securitate socială, adresa de domiciliu, numărul de telefon, data de naștere, informațiile contului de utilizator și parolele.

Metodele de prevenire a unui astfel de atac nu sunt foarte dificile:

- evitarea stocării de informații sensibile care nu sunt necesare;
- utilizarea SSL și securitate HTTPS pe paginile web care **stochează** informații; folosirea unor algoritmi criptografici puternici;
- folosirea unor parole suficient de complexe.

Cross-Site Scripting (XSS)

- Atacurile de tip Cross-Site Scripting (XSS) apar atunci când un atacator folosește o aplicație web pentru a trimite cod rău intenționat, în general sub forma unui script din partea browserului,

către un alt utilizator final. Defectele care permit acestor atacuri să reușească sunt destul de răspândite și apar oriunde o aplicație web folosește intrarea de la un utilizator în ieșirea pe care o generează fără a o valida sau codifica.

Un atacator poate folosi XSS pentru a trimite un script rău intenționat unui utilizator. Browserul utilizatorului final nu are de unde să știe că script-ul nu ar trebui să fie de încredere și va executa script-ul. Deoarece se consideră că script-ul provine dintr-o sursă de încredere, script-ul rău intenționat poate accesa orice cookie-uri, session tokens sau alte informații sensibile păstrate de browser și utilizate cu site-ul respectiv. Aceste script-uri pot chiar rescrie conținutul paginii HTML [Kir22].

Pentru a evita vulnerabilitățile de scripting între site-uri, există câteva metode, precum:

- Cheat Sheet pentru prevenirea XSS (Cross Site Scripting);
- Fișă de prevenție XSS bazată pe DOM;
- Ghid de dezvoltare OWASP articol despre validarea datelor;
- Ghid de dezvoltare OWASP articol despre phishing.

XML External Entities

- Un atac XML External Entity este un tip de atac împotriva unei aplicații care analizează intrarea XML. Acest atac are loc atunci când intrarea XML care conține o referință la o entitate externă este procesată de un parser XML slab configurat. Acest atac poate duce la dezvăluirea de date confidențiale, refuzul serviciului, falsificarea cererii pe partea serverului, scanarea portului din perspectiva mașinii în care se află analizatorul și alte impacturi asupra sistemului.

Factori de risc:

- Aplicația analizează documente XML;
- Datele contaminate sunt permise în porțiunea de identificare a sistemului a entității, în cadrul declarației de tip de document (DTD);
- Procesorul XML este configurat pentru a valida și procesa DTD;
- Procesorul XML este configurat pentru a rezolva entitățile externe din DTD.

Broken access control

- Controlul accesului impune politica astfel încât utilizatorii să nu poată acționa în afara permisiunilor dorite. Eșecurile duc de obicei la

dezvăluirea neautorizată de informații, modificarea sau distrugerea tuturor datelor sau îndeplinirea unei funcții comerciale în afara limitelor utilizatorului. Vulnerabilitățile comune de control al accesului includ:

- Încălcarea principiului cel mai mic privilegiu sau refuz în mod implicit, unde accesul ar trebui să fie acordat numai pentru anumite capacități, roluri sau utilizatori, dar este disponibil pentru oricine;
- Ocolirea verificărilor de control al accesului prin modificarea adresei URL (modificarea parametrilor sau navigarea forțată), a stării interne a aplicației sau a paginii HTML sau prin utilizarea unui instrument de atac care modifică solicitările API;
- Permitea vizualizării sau editarea contului altcuiva, prin furnizarea de identificare unică a acestuia (referințe directe nesigure la obiecte);Accesarea API cu controale de acces lipsă pentru POST, PUT și DELETE;
- Ridicarea privilegiilor. Acționează ca utilizator fără a fi autentificat sau acționează ca administrator atunci când sunteți autentificat ca utilizator;
- Manipularea metadatelor, cum ar fi reluarea sau modificarea unui simbol de control al accesului JSON Web Token (JWT) sau un cookie sau un câmp ascuns manipulat pentru a ridica privilegiile sau abuzarea invalidării JWT;
- Configurarea greșită a CORS permite accesul la API din origini neautorizate/neîncredere;Forțați navigarea către pagini autentificate ca utilizator neautentificat sau către pagini privilegiate ca utilizator standard.

Controlul accesului este eficient numai în codul de încredere de pe partea serverului sau API-ul fără server, unde atacatorul nu poate modifica verificarea controlului accesului sau metadatele, cu excepția resurselor publice, refuzați în mod implicit.

- Implementați mecanismele de control al accesului o dată și reutilizați-le în întreaga aplicație, inclusiv minimizând utilizarea partajării resurselor între origini (CORS);
- Controalele de acces la model ar trebui să impună proprietatea înregistrărilor, mai degrabă decât să accepte că utilizatorul poate crea, citi, actualiza sau șterge orice înregistrare;

- Cerințele unice privind limita de afaceri pentru aplicații ar trebui să fie impuse de modelele de domeniu;
- Dezactivați listarea directoarelor serverului web și asigurați-vă că metadatele fișierelor (de exemplu, .git) și fișierele de rezervă nu sunt prezente în rădăcinile web;
- Înregistrați eșecurile de control al accesului, alertează administratorii atunci când este cazul (de exemplu, eșecuri repetate);
- Limitați accesul la API și la controler pentru a minimiza daunele cauzate de instrumentele de atac automatizate;
- Identificatorii de sesiune cu stat ar trebui să fie invalidați pe server după deconectare. Tokenurile JWT fără stat ar trebui să fie mai degrabă de scurtă durată, astfel încât fereastra de oportunitate pentru un atacator să fie minimizată. Pentru JWT-uri cu durată mai lungă de viață, este foarte recomandat să urmați standardele OAuth pentru a revoca accesul.

Security Misconfiguration

- Aplicația poate fi vulnerabilă dacă aplicația este:
- Lipsește consolidarea corespunzătoare a securității în orice parte a stivei de aplicații sau permisiunile configurate incorect pentru serviciile cloud;
- Funcțiile inutile sunt activate sau instalate (de exemplu, porturi, servicii, pagini, conturi sau privilegii inutile);
- Conturile implicite și parolele lor sunt încă activate și neschimbate;
- Gestionarea erorilor dezvăluie utilizatorilor urme de stivă sau alte mesaje de eroare prea informative;
- Pentru sistemele actualizate, cele mai recente caracteristici de securitate sunt dezactivate sau nu sunt configurate în siguranță;
- Setările de securitate din serverele de aplicații, cadrele de aplicații (de exemplu, Struts, Spring, ASP.NET), bibliotecile, bazele de date etc., nu sunt setate la valori securizate;
- Serverul nu trimite anteturi sau directive de securitate sau nu sunt setate la valori securizate;
- Software-ul este învechit sau vulnerabil (consultați A06:2021-Componente vulnerabile și învechite);
- Fără un proces concertat și repetabil de configurare a securității aplicațiilor, sistemele sunt expuse unui risc mai mare.

Ar trebui implementate procese de instalare sigure, inclusiv:

- Un proces de întărire repetabil face rapidă și ușoară implementarea unui alt mediu care este blocat corespunzător;
- Mediile de dezvoltare, QA și producție ar trebui să fie toate configurate identic, cu acreditări diferite utilizate în fiecare mediu. Acest proces ar trebui să fie automatizat pentru a minimiza efortul necesar pentru a crea un nou mediu securizat;
- Platforma să fie minimală fără caracteristici, componente, documentație și mostre inutile.
- Eliminați sau nu instalați caracteristici și cadre neutilizate;
- Sarcina de revizuire și actualizare a configurațiilor adecvate pentru toate notele de securitate, actualizările și corecțiile ca parte a procesului de gestionare a corecțiilor;
- Examinați permisiunile de stocare în cloud ;
- Arhitectura de aplicație segmentată oferă o separare eficientă și sigură între componente sau chiriași, cu segmentare, containerizare sau grupuri de securitate în cloud (ACL);
- Trimiterea directivelor de securitate către clienți, de exemplu, Antete de securitate;
- Un proces automat pentru a verifica eficacitatea configurațiilor și setărilor în toate mediile.

Insecure deserialization

- Acest tip de atacare are loc atunci când datele controlabile de utilizator sunt deserializate de către un site web. Acest lucru îi permite unui atacator să manipuleze obiecte seriale pentru a trece date dăunătoare în codul aplicației.

Este chiar posibil să înlocuiți un obiect serializat cu un obiect dintr-o clasă complet diferită. În mod alarmant, obiectele din orice clasă care este disponibilă pentru site-ul web vor fi deserializate și instanțiate, indiferent de clasă așteptată. Din acest motiv, deserializarea nesigură este uneori cunoscută ca o vulnerabilitate de „injectare a obiectelor”.

Dacă este necesară deserializarea datelor din surse nesigure, a se include măsuri pentru asigurarea că datele nu au fost modificate. De exemplu, se poate implementa o semnătură digitală pentru a verifica integritatea datelor. Cu toate acestea, orice verificări trebuie să aibă loc înainte de a începe procesul de deserializare.

Dacă este posibil, ar trebui total evitată utilizarea caracteristicilor generice de deserializare. Datele serializate din aceste metode conțin toate atributele obiectului original, inclusiv câmpurile private care pot conține informații sensibile. În schimb, se

pot crea propriile metode de serializare specifice clasei, astfel încât să se poată controla câmpurile care sunt expuse.

Using Components with Known Vulnerabilities

- Atacatorii pot exploata vulnerabilitățile cunoscute ale componentelor într-o varietate de moduri. De exemplu, aceștia pot folosi o vulnerabilitate pentru a obține acces la datele sensibile stocate în aplicație sau pentru a executa cod arbitrar pe serverul aplicației. De asemenea, aceștia pot folosi vulnerabilități pentru a lansa atacuri de refuzare a serviciului (DoS) sau pentru a-și escalada privilegiile în cadrul aplicației.

Un vector de atac comun pentru exploatarea vulnerabilităților cunoscute în componente este atacul lanțului de aprovizionare. Într-un atac al lanțului de aprovizionare, atacatorii vizează o componentă terță parte care este utilizată în dezvoltarea unei aplicații. Prin compromiterea codului sau a infrastructurii componentei, atacatorii pot injecta cod rău intenționat în aplicație și pot obține acces la date sensibile.

Atenuarea riscurilor de utilizare a componentelor cu vulnerabilități cunoscute necesită o combinație de bune practici de securitate și implementarea controalelor de securitate. Iată câțiva pași care pot ajuta la atenuarea riscurilor:

- Actualizați în mod regulat și corectează componentele: dezvoltatorii ar trebui să verifice în mod regulat avizele de securitate legate de componentele pe care le folosesc și să aplice actualizări și corecții cât mai curând posibil;
- Utilizați numai componentele necesare: dezvoltatorii ar trebui să utilizeze numai componente care sunt necesare pentru aplicație și să evite utilizarea componentelor care au un istoric de vulnerabilități;
- Utilizați un instrument de analiză a compoziției software (SCA): instrumentele SCA pot ajuta la identificarea vulnerabilităților cunoscute în componente și pot oferi recomandări pentru remediere; Implementați controale de securitate: dezvoltatorii ar trebui să implementeze controale de securitate, cum ar fi validarea intrărilor și codificarea ieșirilor, pentru a reduce impactul vulnerabilităților și a preveni atacurile;
- Efectuați teste de securitate: testarea de securitate ar trebui să fie efectuată pe aplicație pentru a identifica vulnerabilitățile și pentru a se asigura că vulnerabilitățile cunoscute ale componentelor au fost abordate.

Insufficient logging & monitoring

- Înregistrarea și monitorizarea insuficientă nu reprezintă o vulnerabilitate sau o amenințare directă, ci mai degrabă organizația este oarbă la atacurile active curente, atacurile anterioare și informațiile necesare în procesul criminalistic pentru a determina impactul atacului. Fără această perspectivă, organizația este vulnerabilă la atacuri viitoare prin aceleași metode sau uși din spate plantate în atacurile anterioare, care ar putea fi și mai greu de detectat.

Impactul variază în funcție de tipul de afaceri pe care o desfășoară organizația, dar câteva exemple care pot fi identificate sunt:

- Un comerciant cu amănuntul ar putea avea informații despre clienți expuse, linii noi de produse scurse sau marfă furată.
- Un producător ar putea avea lanțurile de aprovizionare întrerupte, logistica modificată sau sistemele CAM întrerupte.
- O bancă ar putea avea informații despre titularul de cont modificate sau șterse, sistemele financiare întrerupte sau integrarea partenerilor compromisă.

Pentru a atenua înregistrarea insuficientă și monitorizarea, organizațiile trebuie să se asigure că atât jurnalele aplicațiilor, cât și ale tranzacțiilor sunt păstrate și securizate în sisteme separate de stocare și analiză a datelor. Toate sistemele din calea de solicitare/răspuns a API-ului trebuie să își trimită informațiile de jurnal către un sistem de stocare separat, astfel încât să poată fi corelate în timpul criminalisticii. Dacă un sistem API este compromis, atunci informațiile criminalistice stocate pe acel sistem nu pot fi de încredere. Există multe opțiuni care facilitează colectarea informațiilor din jurnal, dar este important de subliniat faptul că fluxul de informații trebuie să fie unidirecțional. Datele dintr-un sistem compromis nu trebuie să aibă permisiunea de a modifica datele deja trimise către sistemul de stocare și analiză, astfel încât implementările care folosesc o unitate partajată sau instrumente precum rsync ar trebui evitate, deoarece manipularea sistemului compromis va schimba datele de pe sistemul de stocare.

În concluzie, în secolul 21 tehnologia este într-o continuă dezvoltare și devine din ce în ce mai utilizată, iar astfel tot mai multă lume primește acces la aceasta. Acest fapt aduce după el atât beneficii, cât și pericole. Este, într-adevăr, foarte util și comod ca tehnologia să lucreze pentru oameni și să le ușureze acestora munca, însă, nu trebuie trecut cu vederea faptul că tehnologia

lucrează prin Internet, iar acesta este plin de pericole. Informațiile din companie sau chiar cele personale pot ajunge pe mâna atacatorilor, fapt care ar produce foarte multe daune economice, sociale, morale. Așadar, în momentul în care se alege expunerea datelor prin internet, trebuie conștientizate pericolele și luate măsuri de securitate cibernetică.

Pentru a veni în ajutorul persoanelor care nu dețin o educație solidă în privința securității cibernetică, există mai multe tutoriale de învățare. Acestea conțin informații cu privire la testări care se pot face în rețea, pe mașina de lucru sau chiar pe site-ul web, pentru a descoperi vulnerabilitățile acestora și a studia apoi modul în care se pot remedia.

Dicționar de cuvinte privitoare la amenințările informatice

MALWARE = prescurtarea de la "malicious software", se referă la orice software rău-intenționat (malițios) creat cu scopul de a rula în mod neautorizat și ascuns față de utilizatorul computerului.

TROIAN = un program malware care este adesea prezentat utilizatorului ca un program legitim, utilizatorul fiind păcălit să descarce și execute aplicația malițioasă pe computerul său. Odată activat, troianul permite atacatorului să controleze și să monitorizeze calculatorul victimei sau să acceseze informații sensibile (parole, poze, etc) stocate pe acesta.

KEYLOGGER = Înregistratoarele de taste sunt programe destinate înregistrării tastelor apăsate de către utilizator și folosite, de pildă în troieni, pentru a obține informații sensibile ca parole, coduri PIN, numere de carduri, etc. Aceste programe rulează în background și sunt *invizibile* pentru un utilizator obișnuit. Ele pot fi instalate pe un calculator în urma unui atac de tip "*drive-by-download*" sau pot fi instalate împreună cu programele piratate.

ADWARE = formă de malware care descarcă sau afișează anunțuri nedorite când utilizatorul navighează online, colectând date de marketing sau alte informații fără știrea utilizatorului și redirecționează căutările utilizatorului către diferite websiteuri ce afișează anunțuri publicitare. Ele se instalează de obicei automat cu unele programe gratuite instalate de pe Internet sau vin la pachet cu programele piratate.

DRIVE-BY DOWNLOAD = descărcarea fără știința utilizatorului și fără ca acesta să observe, pe computer sau pe mobil, a unor

programe malițioase. De obicei un astfel de atac reușește datorită lipsei actualizărilor de securitate, ale browserului sau ale sistemului de operare.

MAN-IN-THE-MIDDLE = Un atac sofisticat în care atacatorul se interpune ca "stație de tranzit" în comunicația dintre două sisteme, utilizatorul legitim "având impresia" că cele două sisteme discută direct, când de fapt atacatorul controlează toată conversația, interceptând și modificând mesajele schimbate de cele două părți. Astfel se pot modifica, de exemplu, date ale unor tranzacții financiare.

MAN-IN-THE-BROWSER = un tip de atac prin care un troian de tip proxy infectează un browser web folosindu-se de vulnerabilitățile de securitate ale browser-ului. Troianul modifică pagini web, elemente ale unei tranzacții sau chiar întreaga tranzacție, toate aceste acțiuni având loc "în background", fără ca utilizatorul să observe. Un astfel de atac ar putea fi contracarat prin utilizarea unei metode de verificare a tranzacției care să folosească un "canal", adică un alt mediu de transmisie, de exemplu SMS, diferit de cel care a fost utilizat pentru inițierea tranzacției, cum ar fi rețeaua web.

Tatiana Dorsescu, Curs de E-business, cap. Securitatea în internet

www.bancatransilvania.ro

www.cec.ro

www.eximbank.ro

www.raiffeisen.ro

www.politiaromana.ro

Mohmed Hassan Nasr, "E-PAYMENT SYSTEMS RISKS, OPPORTUNITIES AND CHALLENGES FOR," International Journal of Intelligent Computing and Information Science, vol. 20, no. 1.

<https://www.globenewswire.com/en/news-release/2022/09/19/2518187/0/en/With-24-4-CAGR-Digital-Payment-Market-Size-worth-USD-19-89-Trillion-in-2026.html>

<https://www.rapyd.net/blog/online-payment-processing/>

V.a.M.E.P.System, "M. Bellare, University of California, San Diego," Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998

<https://noda.live/ro/articles/procesator-de-plati-online>

<https://payproglobal.com/ro/raspunsuri/>

Dumitraș Adelina-Veronica: Studiu asupra plăților electronice, UTCN Intern, 2023

<https://portswigger.net/web-security/xxe>
<https://www.acunetix.com/blog/articles/what-is-insecure-deserialization/>
<https://code-maze.com/owasp-top-10-sensitive-data-exposure/>
<https://www.contrastsecurity.com/glossary/broken-authentication>
<https://tyk.io/blog/res-owasp-api-security-10-insufficient-logging-monitoring/>
https://medium.com/@aakashyap_42928/using-components-with-known-vulnerabilities-cde7a4ec3e62
<https://portswigger.net/web-security/deserialization>
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
https://owasp.org/Top10/A01_2021-Broken_Access_Control/
[https://owasp.org/www-community/vulnerabilities/XML_External_Entity_\(XXE\)_Processing](https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing)
Bontea Ramona: Proiect studiu referitor la posibile vulnerabilități în zona de online și propuneri de metode de evitare, UTCN Intern, 2024

VI. Content Management Systems (CMS)

Un sistem de administrare de conținut (CMS) este o aplicație soft, sau un set de programe care conlucrează pentru a crea și a administra conținut digital. Din punct de vedere lingvistic, un administrator de conținut este orice sistem care te ajută la crearea, stocarea, indexarea, arhivarea, publicarea și distribuția de conținut.

Dintre funcțiile unui sistem de management de conținut menționăm:

- indexare intuitivă, funcții pentru căutare și găsim care să indexeze datele pentru un acces ușor, care să dea posibilitatea utilizatorului de a căuta informații după atribut, cum ar fi data de publicare, cuvinte cheie sau autori;
- administrarea formatului documentelor care să transforme hârtia scanată și documentele electronice în documente html sau pdf;
- funcții de revizuire care să permită conținutului să fie actualizat și editat după publicarea sa inițială; posibilitatea de tracking a modificărilor făcute asupra unui document de către utilizatori individuali;

- funcție de publicare, care să permit utilizarea unui template aprobat de către organizație, precum și alte unelte pentru crearea sau modificarea de conținut.

CMS trebuie să furnizeze instrumente pentru marketingul de tip unu la unu, adică abilitatea unui site de a-și adapta conținutul și reclamele specific pe profilul utilizatorului, folosind informațiile furnizate de acesta (de exemplu cuvinte cheie la căutare). Un sistem de content management ar fi bine să aibă help online integrat, poate chiar grupuri/forum de discuții, sisteme de permisie bazate pe accesul de grup, template-uri care să permită customizarea, adică adaptarea lor de către utilizator, proceduri facile de instalare, suport în mai multe limbi, oferirea unei ierarhii de conținut cu dimensiune și adâncime nelimitată de stocare, cerințe minimale pentru server, administrator de fișiere integrat, precum și jurnale de audit.

Alte funcționalități de care o organizație trebuie să țină cont în alegerea unui sistem CMS corespunzător, ar fi o interfață de editare ușor de folosit precum și capacitate inteligentă de căutare.

De exemplu dacă compania este mare și este întinsă din punct de vedere geografic, administratorul CMS trebuie să știe cam câte persoane vor folosi aplicația, dacă va fi nevoie de suport pentru mai multe limbi străine și cât de mare ar trebui să fie echipa care să furnizeze asistență pentru o bună funcționare. De asemenea trebuie cunoscut nivelul de control(drepturile) atât pe partea administratorilor cât și a end-userilor. Pe lângă acestea trebuie ținut cont de diversitatea datelor din companie, în format electronic precum și de faptul că, orice conținut digital ar trebui să poată fi indexat.

Ca și ofertă de CMS pe piață, există atât oferte gratuite cât și bazate pe abonament, disponibile pentru uz personal sau pentru firme. Iată câteva exemple de astfel de platforme:

- **SharePoint** – este o colecție de tehnologii bazate pe web și cloud care oferă facilități de stocare, distribuire și administrare de informație digitală în cadrul unei organizații;
- **M-Files** – este o abordare bazată pe etichete meta (meta-tags) de administrare a documentelor electronice;
- **Joomla**;
- **WordPress** – WCMS gratuit și open source, bazat pe PHP și MySQL; poate fi utilizat ca și parte a unui serviciu de internet hosting(WordPress.com) sau poate fi descărcat pe un calculator local și să acționeze ca un web server local

(WordPress.org). Acest mediu este foarte popular în rândul bloggerilor;

- **Oracle WebCenter;**
- **Backdrop CMS** - mediu gratuit, open source, parte a proiectului Drupal, concentrat pe proiecte ale organizațiilor mici și medii; sunt oferite trăsături bazice de administrare de conținut, dar se poate extinde prin foarte multe module.

Securitatea CMS

La CMS trebuie avut în vedere un echilibru delicat între securitate și utilizabilitate sau funcționalitate. Acest lucru este important pentru proiectanții de asemenea sisteme pentru a proteja companiile de eventuale riscuri. Din perspectiva programatorului, un CMS este o arhivă, o colecție share-uită. Este o locație virtuală unde anumite persoane dar și procese stochează și găsesc informații, reprezentate ca și fișiere în format digital. Acestea sunt definite și menținute printr-o structură ierarhică. Securitatea conținutului în cadrul unui CMS se poate păstra prin autentificarea persoanelor care accesează arhiva și prin autorizarea conținutului pe care utilizatorii îl accesează precum și a acțiunilor pe care aceștia au dreptul să le facă asupra fișierelor.

Autentificarea utilizatorilor poate avea loc prin formule cum ar fi nume de utilizator și parolă, până la autentificare în doi pași și/sau verificări de natură biometrică.

În ce privește autorizarea persoanelor asupra unui conținut, aceste acțiuni se referă de exemplu la faptul că, cei care scriu pot crea și updata texte noi, editorii pot să le editeze iar cititorii să le vizualizeze. Este util ca fiecare pas să fie cât mai transparent posibil. Nu ar fi de dorit ca fiecare să se autentifice manual de fiecare dată și să caute posibilitățile de autorizare înaintea fiecărei acțiuni pe care ei trebuie să o urmeze. Aceste facilități adaugă valoare unui CMS.

Un asemenea sistem trebuie să ofere un mediu sigur verificând securitatea pentru:

- Zona de perimetru – utilizatorii și procesele au permisia de a accesa și modifica articole din cadrul arhivei în limitele în care cel care a realizat sistemul, le permite. CMS definește un set de roluri, cum ar fi cele de scriitor, editor și cititor, și asignează în mod automat indivizilor rolurile în timpul autentificării;

- Operații permise – se autorizează operațiile printr-un set de liste de control al accesului, determinând cine poate citi, edita, crea sau șterge articole în cadrul arhivei. Mapează rolurile determinate de autentificarea operațiilor, administrând acțiuni legate de conținut;
- Succesiune – listele de control al accesului definesc drepturi ierarhice de succesiune. De exemplu o persoană autorizată să vadă un fișier poate automat să citească toate articolele din cadrul acelui fișier, dacă nu există articole cu permisiuni aparte. Accesul operațiilor autorizate sunt de asemenea ierarhice, o persoană cu drepturi de editare poate citi fișierul dar nu poate crea unul nou;
- Securitate la nivel de articol – de exemplu o companie are nevoie de specificații de design care să fie confidențiale și să fie sigură că doar anumiți ingineri cu grad mai înalt ierarhic pot accesa sau modifica aceste articole. Pentru aceste cazuri există securitatea la nivel de articol. Un CMS poate menține securitatea prin criptarea unor fișiere individuale, sau a unui grup de fișiere, stocate în cadrul arhivei. Tehnicile de criptare cu cheie publică sau privată sunt cele mai răspândite.

Astfel, în echilibrul dintre securitate și funcționalitate, trebuie avut în vedere faptul că , dacă sunt prea multe verificări de siguranță poate fi afectat procesul de lucru, dar dacă sistemul nu este suficient de sigur, pot apare anumite riscuri de scurgere de informație. Astfel, s-au dezvoltat trei proceduri care să echilibreze aceste activități. În primul rând trebuie avută în vedere evaluarea riscurilor printr-un audit legat de informațiile implicate. Este importantă catalogarea tipului de conținut în interiorul CMS, de văzut cât de valoroasă este informația pentru companie și ce riscuri ar apărea dacă unul sau mai multe articole ar ajunge în afara organizației. De exemplu instrucțiunile de utilizare pentru un anumit produs are o valoare diferită față de specificațiile de design ale unui prototip de produs. Este bine a se face o listă cu tipurile de documente care trebuie administrate precum și liniile de afaceri cărora aceste documente aparțin. Este important din perspectiva de business, nivelul de securitate necesar pentru fiecare tip. Aici ar fi utilă sistematizarea într-un tabel a informațiilor cu rubrici legate de tipul de conținut, proprietari, roluri și acțiuni permise asupra acestor date.

Autentificarea la intrarea și accesul la date trebuie să fie suficient de puternică pentru riscurile identificate dar și transparentă pentru utilizator. Aceasta începe de la nivelul de întreprindere, organizație, unde, la majoritatea există un director cu un singur nivel de sign-in, astfel ca un singur set de informații de acreditare permit accesul la multiple resurse de sistem, inclusiv la CMS. Sistemul de securitate ar trebui să includă posibilitatea de recuperare a parolei, dar și autentificare în doi pași, biometrică sau acces sigur de pe mobil.

Trebuie avut în vedere că pot fi diferite situații la care să fie nevoie de unul sau două niveluri de securitate, cum ar fi verificarea personală în cadrul întreprinderii necesară de exemplu designerilor care trebuie să aibă acces la implementarea specificațiilor de prototip pentru un produs nou, informații care nu trebuie să fie accesibile tuturor angajaților.

Autorizare adaptivă – odată ce utilizatorii se autentifică pentru a avea acces la depozitul de date, au permisiunea de a efectua diverse operații specifice asupra conținutului. CMS administrează accesul spre diferitele fișiere, inițial într-o maniera ierarhică, în sensul în care, dacă ai acces la un director, ai acces la toate fișierele din acel director, aceasta dacă nu se specifică altfel.

Sistemele CMS, atât cele cu proprietate cât și cele cu open access se bazează pe permisiuni ierarhice. Însă nu toate permisiunile de acces sunt strict ierarhice, deoarece este esențial să existe flexibilitate pentru aceste sisteme și posibilitatea de a fi adaptate urgent pentru diferite situații speciale, dacă este cazul. De asemenea trebuie avute în vedere situațiile de acces de pe diverse dispozitive, de exemplu dacă un inginer de design intră de pe laptopul său, să aibă posibilitatea să acceseze fișiere de proiectare și să modifice specificații de produs, dar un utilizator ce intră de pe telefonul mobil, să poată de exemplu doar să vizualizeze fișiere.

CMS de generația a treia includ de obicei sisteme de administrare de tip online-business, adaptabile pentru nevoile consumatorilor și cele ale business-ului propriu-zis. Un CMS deschis, de exemplu așa cum este Drupal, este valoros în mod special pentru că este foarte flexibil, permite autorizare adaptivă, incluzând definirea rolurilor și a acțiunilor celor care lucrează cu~ și folosesc acest sistem. Oricum, cei care dezvoltă sistemul pot oricând ulterior modifica logica de la baza sistemului, pentru a seta permisiunile după cum este nevoie.

Autorizarea adaptivă este un element modern și vital pentru securitatea de conținut. Sisteme bazate pe reguli sunt înlocuite de medii de tip machine-learning. Totuși riscurile care apar se schimbă în permanență. De aceea este important să se aibă în vedere că securitatea de conținut nu este un element fix. Tehnologiile CMS sunt importante și sistemele de administrarea de conținut trebuie să fie active și cu opțiuni de noutate permanentă astfel încât să facă față concurenței și situațiilor noi care pot să apară. Aici comunitatea pentru platformele WCM open-source sunt bine dezvoltate pe piață, trebuind să ofere opțiuni viabile pentru orice categorie de software de întreprindere (enterprise software).

Conform statisticilor s-a observat că există multe companii care gravitează în jurul sistemelor **CMS open-source**, nu doar din motive de costuri, dar deoarece există o comunitate foarte mare de experți care au portofolii disponibile pentru a fi consultate și accesate, dând astfel organizațiilor posibilitatea de a alege unelte și consultanță specifică pentru ce au nevoie. De asemenea experții susțin că sursele gratuite, oferă transparență totală pentru codul CMS. Pe de altă parte CMS gratuite pot ajuta utilizatorii să găsească o platformă care se pliază pe nevoile lor. Acest lucru poate fi valabil și pentru companii mici care nu își permit să aibă buget pentru investiții mari.

Multe din avantajele programelor open-source, pot deveni dezavantaje în anumite condiții, în funcție de tipul de organizație și de dimensiunea și profesionalismul resurselor IT de care dispune. De exemplu, întreprinderi din domeniul finanțelor sau sănătății, ar putea avea semne de întrebare referitoare la securitatea datelor organizației dacă aceasta este construită pe un sistem CMS open-source. Totodată, s-ar putea ca partea interesantă a codului open-source, aceea de biblioteci vaste de programe extensibile, personalizări sau tipare de tip templates, să fie mai accesibile ca tip de informație celor din domeniul IT cu vastă expertiză, și chiar să nu fie de folos firmelor din alte domenii, care nu se pricep și nu sunt interesate în dezvoltarea interfețelor și a sistemelor de stocare pe care le au, ci doresc doar utilizarea acestora în bune condiții.

“It often comes down to how willing a company is to ... deal with not-so-perfect software,” Liewehr said. “The team needs to be willing to roll up its sleeves and work with the code to address any shortcomings.” În ce privește suportul tehnic, acesta este mai puțin formal în mediul open-source. Dacă ai o întrebare sau o problemă, o

prezinți comunității și speri să obții sau să găsești răspuns. În timp ce, pentru un soft cumpărat, te aștepți să ai mentenanță și ajutor, ori de câte ori este nevoie.

Un alt aspect ar fi logevitatea proiectelor soft. Platformele open-source, uneori apar și dispar, în funcție de cât sunt de interesante pentru cunoscători. De aceea, o companie poate avea nevoie să aleagă fie surse gratuite care au în spate o comunitate activă și bine definită, pentru a asigura managementul pe termen lung, sau să aleagă să plătească o firmă care să se ocupe de aceste aspecte de administrare de conținut.

Legat de costuri, se poate să fie o capcană, și anume că se preia soft gratuit, neștiindu-se din start dacă va fi util firmei, ceea ce poate necesita timp pierdut până să se afle dacă este softul care trebuie sau nu. De asemenea, cine lucrează cu aceste surse gratuite, sunt angajați care trebuie să se priceapă la softurile respective. Și aici există riscul ca angajații să nu aibă calificarea necesară pentru softurile existente. Ca atare, s-ar putea ca prin cumpărarea unui soft cu licență să se obțină o siguranță mai mare și poate per total, costurile să nu fie atât de ridicate cum par inițial.

Un alt aspect întâlnit în ultimii ani este acela în care există o abordare **hibridă**, adică sunt combinate softuri de cost mic cu programe gratuite. Se mai poate ca nu costul să fie factorul hotărâtor, ci tehnologiile care sunt disponibile și care sunt cele mai potrivite firmei din punct de vedere funcțional și nu al costului.

“We’re seeing less and less of a distinction between open source and commercial,” said Tony Byrne, president of Real Story Group. “The differences between them are starting to evaporate. Many of the major open source projects are becoming more commercialized, and vendors can’t argue that they are cheaper anymore.”

Un alt aspect important este acela al **administrării conținutului în cloud**, referindu-se la operații precum colectarea, furnizarea, găsirea, guvernarea și administrarea de informații într-un mediu bazat pe cloud. Asemenea sisteme furnizează întreprinderilor stocarea de date și procese automate pentru monitorizarea de text, imagini, video, audio sau alt conținut multimedia, începând de la creare, editare, organizare, stocare, publicare, arhivare până la ștergere. Serviciile în cloud include de obicei **EDM** (enterprise document management), **WCM** (web content management), web hosting și suport tehnic. Administrarea de conținut în cloud permite cu ușurință echipelor să lucreze împreună și să acționeze simultan

asupra fișierelor și conținutului, să păstreze șirul versiunilor de lucru, conținutul fiind în acest caz accesibil atât pe dispozitive mobile cât și pe desktop. Unele firme care oferă servicii de cloud sunt de sine-stătătoare și specializate pe acest tip de produse, în timp ce altele au integrate servicii de cloud la produse existente tradiționale, instrumente, soft și servicii. Se poate ca organizațiile să folosească sisteme bazate pe ECM în cloud ca o augmentare a activității inițiale, permițând reevaluarea business-ului din perspectivă digitală, creând astfel atât noi oportunități dar și provocări. Procesele de business devin astfel independente de geografie, se pot extinde, angajații pot lucra împreună oriunde s-ar afla pe glob, informațiile sunt astfel disponibile oriunde și oricând. Multe firme au ajuns la soluții de cloud pentru a îmbunătăți și eficientiza procesul comercial, de exemplu sharing-ul de fișiere în cloud înlocuind e-mailul ca transmitător primar de documente, sau cloud-ul înlocuind serverele locale ca mijloace de stocare.

Ca și tip de taxare, se poate ca firma să aibă angajați care să lucreze și să fie interfața pentru gestionarea informației din cloud, sau firmele să fie taxate pe utilizatori sau pe număr de site-uri. Trebuie avute în vedere aspecte ca instalarea, mentenanța unui sistem CMS, furnizarea de soft adus la zi (upgrade) în timp real, tratarea și soluționarea problemelor tehnice și asigurarea securității datelor. Astfel sistemele pot fi mai mult sau mai puțin modulare, site-uri se pot construi sau șterge, trebuind să se aibă în vedere și aceste aspecte de dinamică.

- **Servicii open-source:** acestea sunt de exemplu Drupal sau WordPress, care nu au costuri inițiale dar taxează pentru servicii adiționale premium, cum ar fi suport tehnic, instruire, customizare sau template-uri de conținut.
- **Servicii integrale în cloud:** sunt oferite de firmele specializate și nu permit customizare întotdeauna sau colaborarea pe soft cu alte părți implicate.
- **Servicii hibride în cloud:** chiar dacă serviciile sunt în cloud, permit inmixtiunea unor alte părți implicate, cum ar fi angajații firmei client, pentru customizare sau adăugare de soft.

Sistemele de ECM din cloud sunt viabile, dacă serviciile de securitate sunt bine puse la punct, adaptate atât nevoilor firmei cât și, din punct de vedere tehnic, situației contemporane a aspectelor legate de securitate.

Platforma **iCould Apple** furnizează soluții de administrare de conținut și soluții de stocare care permit file-sharing și controlul pe dispozitive mobile și desktop.

Oracle - este un CMS bazat pe cloud care permite echipelor să colaboreze într-un canal "omnichannel" într-un hub de conținut, pe creare, administrare și publicare de informații. De asemenea asigură servicii de conținut pe aplicații deja existente și integrarea altor instrumente de business.

Alți furnizori de sisteme CMS în cloud ar fi DropBox, OpenText/Documentum, Acquia, Seismic, IBM, Hyland OnBase și M-Files. De asemenea pentru stocare și administrare rudimentară, de bază, se pot folosi și Microsoft OneDrive sau Google Docs.

Acquia

Acquia este o platformă digitală care oferă software și servicii și care, împreună cu Drupal, asigură utilizatorilor și companiilor abilitatea de a crea, opera și optimiza site-uri web, aplicații sau alte experiențe digitale. Este leader în domeniul Digital Experience Platform(DXP) deoarece oferă suport în ce privește cloud computing, administrarea CMS, personalizare și aplicații multi-channel. Este o platformă digitală care susține și ajută comunitatea Drupal pentru a oferi infrastructură, suport și servicii organizaționale, pentru a face accesul la Drupal mai ușor. Inițial, în 2007 când a fost creată, oferea administrare de cloud hosting, dar acum conține și instrumente de marketing și transformare digitală, cu posibilități de business pentru cei din domeniul de marketing, programării și IT.

Versiunea 7.x a Drupal își extinde viața până în noiembrie 2022, dar Acquia dorește să acopere utilizarea cu succes a Drupal 7.x până în 2025, furnizând actualizări la zi pe platforma Acquia Cloud. Acquia include de asemenea standarde la zi de securitate web astfel încât utilizatorii să aibă site-uri sigure.

Acquia Dev Desktop furnizează modul cel mai sigur și mai rapid pentru configurarea și rularea Drupal pentru dezvoltare locală(pe computer) pentru sisteme Mac sau PC. Acquia Dev Desktop este un DAMP stack installer, adică deține și oferă toate componentele necesare pentru rularea locală a unui site, și anume Apache, MySQL și PHP. Deoarece are integrare pe platforma Cloud, prezintă metoda cea mai ușoară de a publica, dezvolta și sincroniza site-urile Drupal locale pe web.

Componente ale Acquia Dev Desktop:

Server HTTP Apache	Cel mai popular web server din lume
Server MySQL de baze de date	Percona Server, cel mai popular pe baze de date, având performanțele cele mai bune
PHP	Limbajul care stă la baza Drupal
phpMyAdmin	Instrument pentru administrarea in-browse a bazelor de date
Xmail Server (doar pe Windows)	Permite site-ului instalat local să trimită email-uri direct, ceea ce este important pentru resetarea parolei, testării și a altor proprietăți

Instalarea se poate face ținând cont de indicațiile de mai jos

<https://docs.acquia.com/dev-desktop/>

unde, versiunile Drupal pentru care în prezent funcționează ar fi Drupal 8 și 9.

Drupal – Privire de ansamblu

Drupal este un mediu gratuit CMS (Content Management System) de tip open source care permite organizarea, gestionarea și publicarea de conținut. Este realizat pe baza unor medii PHP, sub licența GNU (General Public License), ceea ce face ca oricine să aibă permisiunea de a descărca și de a distribui surse și tot ceea ce ține de acest sistem. Iată câteva site-uri care folosesc Drupal pentru gestionarea de conținut online: WhiteHouse.gov, World Economic Forum, Stanford University etc.

După cum se preciza și mai sus, un CMS, adică un sistem de gestionare de conținut, practic se ocupă de stocarea de date, cum ar fi text, muzică, fotografii sau alte tipuri de fișiere, de editarea, publicarea și modificarea acestora, precum și de prezentarea pe site a întregului conținut.

Prima variantă standard Drupal este lansată în ianuarie 2001, de către Dries Buytaerti și este considerată ca fiind dominantă pentru mai multe tipuri de afaceri. Un mare avantaj al Drupal ar fi faptul că este mult mai flexibil decât alte CMS și permite construcția de site-uri complexe, mari. Acest sistem conține structuri predefinite bazate pe

PHP = unul dintre limbajele importante de programare web, deoarece are versiuni pentru majoritatea tipurilor de servere și sistemelor de operare, fiind un limbaj open-source și server-side.

Unul din avantajele este acela că permite crearea de pagini și adăugarea de conținut fără ca utilizatorul să fie nevoit să aibă cunoștințe tehnice de web design, HTML sau alte limbaje de programare. Bineînțeles că poate fi apoi dezvoltat și customizat într-un mod profesional, cu ajutorul cunoștințelor de PHP și HTML, dar nu este neapărat nevoie de acestea într-o primă fază. În funcție de necesitățile utilizatorului, există module specializate pentru diferite tipuri de operații și pentru dezvoltarea sau rafinarea acestora. În decembrie 2019, existau cca 44000 module.

Drupal –Proprietăți specifice

Site-urile sunt ușor de creat și de întreținut
Poate adapta orice la sistemul existent prin interfețe built-in
Realizează conexiunea site-ului prezent la alte site-uri și servicii prin facilități de search engine sau feeds
Este un software open source, deci gratuit
Poate crea un site foarte flexibil și cu o prezentare vizuală de calitate, ajutând astfel la creșterea numărului de vizitatori pe site
Poate publica conținutul paginii tale în Social Media (de ex Twitter, Facebook etc)
Permite utilizarea de teme customizabile de design și punere în pagină de conținut
Conținutul poate fi administrat de către Drupal, putând fi prezentat pe site-uri social media, de informații, intranet sau alte aplicații web

Avantaje

CMS flexibil, permițând manipularea de conținut de tip text, video, audio, blog, meniu, statistici etc
Deoarece conține teme predefinite, designul site-ului practic nu este pomit de la zero
Este ușor de administrat în cazul creării de pagini web sau blog, conținutul fiind ușor de organizat și de reutilizat
Și-a dezvoltat o securitate destul de bună
Există o comunitate foarte mare de programatori profesioniști în acest domeniu
Temele de design predefinite dau paginii o formă plăcută și atractivă
Se pot crea plug-in-uri personalizate, însă Drupal oferă din start peste 7000 de aplicații deja existente care se pot doar folosi

Plug-in = sisteme native de interfață asemenea PHP, cu proprietatea că sistemul plugin poate descoperi orice implementare pe o interfață, lucrează cu metadata și furnizează crearea și existență de clase. Diferite tipuri comportamentale ale acestora sunt implementate prin interfețe comune. Altfel spus, sunt module sau subsisteme care furnizează funcționalitate într-un mod extensibil, orientat pe obiecte; pentru funcționalitate există ca bază interfața, iar alte module pot crea/implementa plugin-uri cu diferite tipuri de comportament (de exemplu prelucrare de imagini – scalare, saturare, decupare etc).

Dezavantaje

Nu are o interfață foarte prietenoasă. Necesită totuși anumite cunoștințe de bază pentru a putea instala platforma și a face modificări pe aceasta
--

Este un CMS de sine-stătător, nefiind compatibil cu alte platforme soft

Nu are performanță ridicată, încarcă destul de mult serverul și nu se va deschide dacă există o conexiune de internet foarte lentă
--

CMS sunt de obicei folosite pentru **ECM** (Enterprise Content Management- administrare de conținut al unei organizații) și **WCM** (Web Content Management – administrare de conținut web). CMS trebuie să permită unui utilizator non-tehnic să poată administra orice bun pe un site cu care acesta dorește să interacționeze, indiferent despre ce tip de conținut este vorba: text, poză, video, informație extrasă din alte surse, etc.

ECM / WCM

În cadrul companiilor mari, numărul de documente fizice și electronice este în continuă creștere, astfel încât devine tot mai greu ca aceste documente să fie găsite sau organizate într-un mod eficient. În lipsa unei bune organizări, documentele se pot pierde în email-uri, se pot rătăci prin directoarele de pe calculator sau pot fi accesate greu în arhive, dacă acestea nu sunt eficient scanate și organizate. Toate acestea pot duce la inconveniente cum ar fi încetinirea fluxului de date în cadrul organizației. **ECM** (Enterprise Content Management) trebuie să furnizeze o soluție software pentru administrarea și gestionarea conținutului de informații ce include gestiunea documentelor, fluxul de lucru, raportarea și notificările, depinzând de specificul companiilor din care acestea fac parte. Pentru organizații acest sistem este necesar pentru reducerea de costuri și îmbunătățirea productivității, permițând accesul rapid la documentație, un proces de afaceri automatizat care să răspundă în timp cât mai scurt la cererile clienților. Din punctul de vedere al

utilizatorilor, este important timpul scurt și efortul minim pentru organizarea, găsirea și gestionarea de documente, prin folosirea unui motor puternic de căutare.

În principal, managementul eficient al documentelor se realizează prin operațiuni ca:

- Organizarea și schimbul documentelor electronice
- Scanarea documentelor de hârtie în DMS (Document Management System)
- Alocarea de meta-datelor (indexare)
- Clasificarea documentelor în funcție de conținut
- Clasificarea documentelor și a notelor frecvent vizualizate
- Automatizarea proceselor de afaceri (cerere de schimbare, revizuire și aprobare a documentelor)
- Controlul accesului la documente (până la 9 niveluri de protecție)
- Accesul și editarea documentelor
- Ușurință în căutarea documentelor prin căutare rapidă sau detaliată
- Indexare și vizualizare a mai multor versiuni ale aceluiași document
- Crearea de rapoarte pe baza documentelor
- Gestionarea dosarelor cu mai multe documente
- Posibilitatea de a crea documente în aplicații consacrate: MS Office (Word, Excel, Outlook, Power Point etc.), Lotus mail, etc. și încărcarea în DMS (Document Management System), online, utilizând opțiunea drag&drop.

ECM (Enterprise Content Management) – este un set de procese, strategii și unelte care permit unui business să obțină, să organizeze, să stocheze și să furnizeze informații decisive către angajați, acționari și clienți. Acest sistem are ca rol simplificarea furnizării de informații, administrarea de documente și fluidificarea fluxului proceselor automate. Sistemul trebuie să fie compatibil cu formularele care conțin evidența productibilității companiei fișiere cu imagini, email, CAD și altele.

Atât ECM cât și WCM sunt sisteme CMS. Diferența majoră este însă aceea că, ECM lucrează intern în cadrul unei organizații, administrând informația (documente, fișiere) și procesele din interiorul unei organizații, în timp ce WCM se ocupă de publicarea și distribuția informației în exteriorul organizației. Altfel spus, WCM se referă la venituri, la măsurarea succesului în exterior și la maximizarea target-ului iar ECM la profitul net și la eficientizarea procesului intern.

ECM facilitează procesările și colaborările din spațiul de lucru prin integrarea administrării de documente, de active digitale, a funcției de păstrare a înregistrărilor, și furnizând utilizatorilor acces la activele digitale ale organizației.

WCM este util pentru lucrul în colaborare a site-urilor web, fiind dotat cu funcții de publicare, conținute în softul ECM. De obicei însă paginile web ECM rămân după firewall-ul organizației.

WCM se referă la publicarea de conținut pe web, cu specificarea că nu mai este vorba doar despre propria pagină web a unei companii, ci și de publicare în mediul mobil sau pe rețele de socializare gen Facebook.

Atât ECM cât și WCM au două componente:

-CMA= content management application, care este o interfață grafică ce permite utilizatorului să controleze crearea, modificarea și îndepărtarea conținutului de pe un site, fără a avea cunoștințe de html

-CDA=content delivery application care furnizează serviciile back-end care stau la baza administrării și furnizării de conținut, odată ce acesta este creat în CMA.

Beneficiile și importanța ECM

Sistemul ECM furnizează o platformă centralizată în care conținutul poate fi depozitat și diseminat conform unor reguli de conformitate și de securitate. Acest lucru se realizează prin eliminarea proceselor ad hoc care ar expune organizația la riscuri.

Sistemele ECM complet funcționale includ taxonomia de conținut(probleme de clasificare), furnizare de informații specifice pentru audit, integritatea datelor, minimizarea cheltuielilor, controale pentru fluxul de date cu verificare la intrare și ieșire, precum și mecanisme de securitate.

Un sistem optim de management al conținutului poate asigura un acces flux uniform și continuu de date, cu procese de business corespunzătoare acestui flux, strangulările de informații evitându-se prin reducerea înmagazinării datelor și optimizarea proceselor mecanismelor de securitate. Aceste elemente pot duce la creșterea productivității. Softul ECM trebuie să fie capabil să recunoască și să elimine duplicatele dar și să identifice excepțiile.

Pentru început este necesară documentarea pentru a se descoperi toate tipurile de conținut cu care organizația are de a face, toate procesele de business precum și informațiile referitoare la cine

va manipula aceste informații. Sistemele ECM au devenit tot mai importante în ultimii ani, fiind vitale pentru a păstra informațiile fără posibilități de fraude financiare și scurgere de informații, ci pentru protejarea organizației și reputației acesteia. De asemenea aceste structuri trebuie să interacționeze cu aplicații de analiză de business intelligence(transformarea datelor în decizii de business)(BI) și business analytics(BA) pentru a le furniza informații utile pentru luarea de decizii.

BI= business intelligence= transformarea datelor în decizii de business; soluția de BI analizează date și informații actuale și istorice pentru a oferi previziuni precise cu privire la trenduri și evenimente din industria în care se lucrează

BA= business analytics= practica de explorare metodică și iterativă a datelor unei organizații, cu emfază pe analiza statistică; este utilizată pentru luarea de decizii bazate pe un set de date

În prezent, aceste strategii trebuie să se adapteze nevoii de continuă tehnologizare, posibilității de a prelucra în timp real cantități tot mai mari de informație iar platformele ECM trebuie să aibă capabilități de procesare pentru DAM (Digital Asset Management).

Digital Asset Management = administrarea bunurilor/activelor digitale presupune folosirea unei aplicații pe calculator care să facă posibilă organizarea, stocarea, prelucrarea și găsirea fișierelor din activul digital. Aplicația trebuie să se ocupe și de administrarea drepturilor utilizatorilor asupra bunurilor digitale.

Activele din domeniul analogic sau digital sunt transpuse în DAM prin codare, scanare, recunoașterea optică a caracterelor sau prin crearea lor ca obiecte digitale. Acestea pot fi fotografii, muzică, video, animație, podcast și sunt păstrate ca fișiere digitale. La modul cel mai simplu, DAM este o bază de date ce conține metadate despre numele fișierului, formatul său, proprietate și informații despre conținut și modul de utilizare.

O funcție primară a DAM este furnizarea utilizatorilor de indexări după care să se poată face căutarea de conținut și/sau metadate precum și catalogarea acestora. De asemenea ca și caracteristici ar fi accesul facil de oriunde, implementare rapidă, integrare ușoară și trebuie să fie o unealtă intuitivă.

Sistemele de active digitale pot fi de mai multe tipuri. Cele referitoare la brand, conțin informații legate de marketing, cum ar fi logo-ul de exemplu. Cele referitoare la biblioteci se concentrează pe stocarea și regăsirea de bunuri digitale care nu se modifică des, cum

ar fi arhivele foto. Sistemele de administrare de conținut de producție se referă la structuri create pentru producția digitală media, cum ar fi jocurile video. De asemenea există un sistem de cloud care permite utilizatorilor să acceseze conținut de pe orice dispozitiv, inclusiv de pe telefoane mobile.

În prezent, softul pentru administrarea de conținut digital este incorporat în structurile de CMS și sunt de interes pentru companii de retail care au site-uri cu interfață pentru clienți. DAM se consideră a fi o subunitate a ECM.

Folosind DAM, specialiștii de marketing își pot dezvolta firma și crește consistența brandului, designerii pot avea un flow de lucru mai facil printr-o căutare rapidă a surselor digitale cu care lucrează, echipele de vânzări au update în timp real la materiale și resurse, organizațiile își păstrează fișierele organizate iar distribuitorii își optimizează procesul de livrare.

Podcast= fișier digital audio disponibil pe internet pentru a fi descărcat pe un calculator sau pe un media player portabil.

Din punct de vedere istoric, noțiunea de ECM (Enterprise Content Management) a apărut în urmă cu circa 40 de ani, ca o urmare firească a tehnologiei informaționale și a nevoilor din domeniul afacerilor. Este deci un sistem construit unind condiții și necesități tehnologice și de afaceri. Pornește de la faptul că hârtia era greu de distribuit mai multor părți, cu eforturi de cost și de printare/copiere, în timp ce calculatoarele au putut scana documentele și să le stocheze și transmită cu costuri minime. Astfel, hârtia a fost înlocuită cu documentele electronice iar internetul a putut fi folosit ca un mediu de publicare. Prin aceste mijloace, managementul organizațional este fluidizat iar distribuția de informație devine mai rapidă; mediile bazate pe internet pot colabora mai repede și mai ușor iar utilizatorii pot crea conținut într-un mod regulat și securizat, iar acesta poate fi distribuit tuturor, într-o manieră universală. Se salvează astfel timp și bani.

Internetul a creat coeziunea dar totodata și fragmentarea. A făcut globul pământesc mai mic, utilizând protocoale comune. Au dispărut granițele impuse de țări, rase, clase, religie sau altele. Datorită omniprezenței sale, internetul devine o sursă de știință și interacțiune, având însă și slăbiciuni, cum ar fi sursele neverificate/neverificabile, sau rezultatele de căutare dispersate. Astfel, internetul este de fapt nestructurat, nesigur și incontrollabil.

Societatea s-a transformat dintrun consumator, în generator de conținut. În anii '60, când televiziunea a ajuns la marea masă a populației, a existat o dorință nebună de consum a informației, având la acea vreme foarte puțini producători de conținut. În anii '90, odată cu apariția internetului, a fost necesar mai mult și tot mai mult conținut. În 2010, conținutul a fost produs la o rată uluitoare, având la bază doar puține canale, cum ar fi YouTube, Facebook sau Twitter. Dacă societatea a trecut rapid la lucrul cu conținut, organizațiile au făcut mai încet aceste schimbări. Personalul organizațional a fost încurajat să creeze conținut de valoare astfel încât deciziile la nivel corporatist să poată fi luate rapid. Organizațiile au preluat canalele universale folosite de către societate.

Tehnologii colaborative au fost astfel dezvoltate, în forme semnificative cum ar fi wiki, forumuri, asistență, managementul de proiecte sau întâlniri online. Acestea puteau ajunge la un număr mult mai mare de acționari prin intermediul internetului, decât prin fax sau hârtii trimise prin poștă.

Sursele de informații ale unei organizații trebuie să fie auditabile și să asigure acționarilor lor informații exacte, verificate. Pentru luarea de decizii, propuneri de afaceri, informațiile trebuie să fie precise, verificabile, protejând totodată conținutul acestora. ECM ajută la folosirea de structuri de conținut sigure și valide pentru colaborări, dar fără pierderea controlului în manipularea acestora.

ECM

Dacă am considera o definiție simplă a administrării organizaționale de conținut (enterprise content management - ECM), aceasta ar fi gestionarea tuturor formelor de informație în cadrul unei organizații, prin urmărirea de a captura, păstra și furniza informația ca un bun de preț al corporației, într-un mod consistent, natural și reutilizabil, astfel încât organizația să poată susține, dezvolta și rafina investiția sa de cunoștințe.

Pe lângă aspectele de mai sus, ECM se referă și la strategii, metode și unelte aferente care permit administrarea și accesarea informației nestructurate în orice moment în timp și spațiu.

ECM incumbă elemente de strategie și metodologie:

Latura de "**organizație**/antrepriză" se referă la funcțiile de distribuție, aplicare, publicare, achiziție, captură și acces, într-o manieră uniformă și universală. Definește modul în care ECM are efect de **cum și unde?**

Latura de **conținut** descrie componentele semnificative, informațiile, datele structurate sau nesstructurate, înregistrări, fișiere, reguli, structuri, teme și șabloane, tipare. Toate aceste elemente compun ECM. Definește modul în care ECM are efect de **ce**?

Latura administrativă, de **management**, pune laolaltă elementele de comunicare, procese, fluxul de activități, colaborări, interacțiuni și schimburi cu grupul de acționari. Definește modul în care ECM are efect de **cine? când? de ce?**

Ciclul de viață al unui ECM

ECM cuprinde deci strategii, metode și instrumente pentru capturarea, gestionarea, stocarea, păstrarea și furnizarea de conținut, fiind capabil să gestioneze conținutul informațional nestructurat al organizației.

Ciclul de viață al informației conține procesul de **achiziție, stocare și furnizare** de conținut în cadrul organizației. Aceste acțiuni sunt bazate pe factori care țin de întreprindere, conținut și management.

Platforma de unde conținutul este achiziționat sau inițiat este de tip desktop, internet sau fax/email/printer/scanner. Forma de bază a conținutului se poate numi obiect(de conținut).

Achiziția sau captura informației poate fi făcută în cadrul organizației prin desktop, generându-se astfel documente, prin internet care capturează material prin/din aplicații web, sau scanare de documente. Astfel, achiziția în organizație se poate face prin dispozitive multifuncționale care folosesc e-mail-ul pentru distribuție sau un director central cu fișiere pentru depozitare. Aceste resurse vor putea fi accesate și folosite de către persoane care cunosc contextul și conținutul păstrat, pentru a-l putea indexa și cataloga.

Conținutul poate exista în format electronic sau pe hârtie, în urma capturii, el fiind transpus într-un format agreeat de către organizație, pentru a putea fi astfel stocat, acceptat și vizualizat. Catalogarea conținutului este realizată cu resurse calificate, distribuite în cadrul organizației. Aceste surse sunt furnizate de o formă de aplicație electronică ce permite scanarea masivă, indexarea, categorizarea, catalogarea informației pentru a face ulterior posibilă găsirea de conținut. Pe măsură ce acest conținut este vizualizat, el poate fi apoi identificat prin noi proprietăți și atribute, care rezultă în urma tipului și numărului de vizualizări.

Stocarea informației trebuie să fie făcută astfel încât să permită distribuirea, recompunerea ei și livrarea prin cloud. Există

unelte specializate care administrează accesul la arhiva virtuală, care au posibilități de stocare de mari dimensiuni. Stocarea de conținut organizațional, poate fi orice de la rafturi cu dosare pentru documentele originale, la imagini electronice stocate pe un fișier accesibil prin internet.

Sigur că depinde foarte mult tipul conținutului pentru a asigura o arhivare potrivită, pentru a permite mai multe versiuni ale obiectelor de stocat, revizuirii sau suprapunerii de obiecte, pentru a captura tranziția sau modificarea obiectului.

Administrarea arhivelor, versiunile de conținut, controlul asupra drepturilor de autor, cine are drept de modificare sau de distribuție, toate acestea trebuie stabilite pentru ca fiecare utilizator care are acces la arhive să poată accesa atât cât îi permite statutul său. Arhivarea trebuie să permită și extinderea capacității de stocare, stabilirea ciclului de viață de conținut, astfel încât arhivele să poată fi distruse la momentul potrivit, dacă este nevoie.

Livrarea de conținut organizațional, include instrumente de *căutare* și *publicare*. Căutarea se consideră un mecanism de furnizare a informației deoarece informația este găsită pe rând, nu toată odată.

Publicarea distribuită are costuri diferite în funcție de specificitatea afacerii respective și în funcție de criteriile stabilite prin care conținutul va fi distribuit prin anumite căi bine stabilite.

Multe sisteme de administrare de conținut pot să debuteze prin a fi folosite doar de către un singur departament, cum ar fi cel de marketing, financiar sau de reclamații.

Informația poate fi prezentată pe pagina web, inclusă în documente electronice care se pot descărca online, sau furnizate pentru listare. Este importantă aici tehnologia de căutare, mijloacele oferite utilizatorilor pentru a căuta conținutul de publicat sau prezentat cât de repede posibil. Există mecanismul de BPM (business process management) care urmărește acordarea activităților companiei la nevoile și dorințele clienților. Este util pentru definirea și acordarea produselor de soft. Promovează eficiența unei organizații, îmbunătățind activitatea prin flexibilitate și inovație precum și dezvoltarea cu aplicații software. Managementul afacerii prin procese presupune limbajul prin care procesele sunt documentate, măsurate, li se definesc indicatori de performanță și se îmbunătățesc în cadrul organizației. Importanța BPM constă în a oferi un set de elemente și notații unitar, intuitive și ușor de utilizat pentru cei care participă la procesul de livrare.

Procesul de business poate fi definit ca o succesiune de activități ce țin de planul și de domeniul de afaceri pe care participanții, utilizatorii le realizează pentru a atinge obiective propuse și pentru a furniza informație de valoare. Aceste fluxuri de business pot fi în general de management, operaționale sau de suport.

ECM din punctul de vedere al organizației

Pentru o organizație este important să realizeze exact care sunt cunoștințele ei, care este informația importantă pe care o posedă. În acest context, trebuie văzut și conștientizat de ce informația este atât de importantă și trebuie păstrată, cine poate acționa asupra ei pentru a o modifica, unde poate fi aceasta accesată, cine o poate crea și administra, cum se interpretează această informație?

Organizațiile sunt ele însele canale de informație, dobândind-o și generând-o prin intermediul sistemelor, proceselor și a oamenilor.

În varianta cea mai de bază, când toată informația este păstrată pe hârtie, accesarea și modificarea de conținut devine destul de greoaie. Se va pune deci problema de cât de importante și relevante sunt acele date pentru procesele organizaționale și dacă datele trebuie deci păstrate.

Pentru o organizație care este mai mare, canalele de management de informație trebuie să fie dezvoltate pentru a comunica cu mai mulți furnizori, pentru a lucra cu mai multe produse, toate acestea necesitând noi tipuri de conținut cum ar fi imagini pe suport electronic, e-mailuri, fotografii, fișiere CAD, etc. Aici este nevoie de un catalog care să păstreze, să administreze și să modifice acest conținut.

Unele organizații folosesc mai rar anjagați și sisteme pentru procesarea de informații. Aceștia au timpi de reacție mai mari în lucrul cu datele, nepunându-se foarte mare accent pe acesta.

Alte organizații sunt foarte active, producând o cantitate enormă de informație, pe măsură ce lucrează, reacționează în colaborările cu alții și cresc. Acestea se bazează pe productivitatea și motivația angajaților. Supraviețuirea lor este încărcată de riscuri, dar mărimea organizației o face posibilă în ciuda obstacolelor și posibilelor greșeli care apar. Aici este necesar un flux cursiv pentru transmiterea informațiilor, de la front-office la back-office, prin colaborare, coordonare, direcționare a datelor, pentru a evita gâtuirea acestora și fără a periclita bunul mers al organizației.

De exemplu, în industria finanțelor, afacerile sunt gestionate în funcție de cererea de la ghișee (front-office), dar acest lucru se face la birouri (back-office), unde se urmărește ca toate procesele și acțiunile să fie conforme, solvabile și apte de a înregistra toate acțiunile comerciale din front-office.

Organizațiile trebuie să fie responsabile pentru întreaga informație pe care o vehiculează. Trebuie stabilite reguli, algoritmi, limitări pentru clasificarea informației pe care o dețin, totul fiind realizat cu mapare de procese, stocat în depozite de active de conținut și stabilite regulile de afaceri după care organizația funcționează.

De când cu apariția internetului, totul este disponibil marelui public, fără a fi necesară o plimbare la bibliotecă. Motoarele de căutare au în locuit bibliotecarii iar informația a devenit universală. Pe măsură ce se generează tot mai multă informație, crește nevoia de angajare a unor persoane care să fie capabile să extragă, să categorisească și să reorganizeze informația, specialiștii de expertiză trebuind să aibă calificare în diverse domenii, în funcție de natura informației cu care aceștia au de lucru. În acest domeniu s-a făcut un studiu și s-a revelat faptul că, deși persoanele sub 35 de ani sunt mai adaptabile și pot colecta date într-un timp foarte scurt, ele o fac haotic și superficial, nefiind capabile de o categorisire potrivită, deoarece aceste persoane fac parte din generația internetului. Deși pot achiziționa rapid date, le este greu să le rețină și să le compare și categorisească.

ECM definește rolurile pe care organizația trebuie să le asigure, faptul că persoanele corecte sunt angajate pe poziții corespunzătoare pentru ca informația să rămână consistentă și disponibilă. Astfel, cei care se ocupă de arhive, trebuie să aibă în vedere ca informația să fie la zi și corespunzător indexată, designerii trebuie să se asigure că informația existentă și arhivată este relevantă și prezintă un activ, un bun de preț, iar analiștii au sarcina de a îmbunătăți și completa informațiile pentru a detecta trendurile.

ECM trebuie să asigure o administrare optimă de informații, pentru ca organizația să susțină și să recunoască contribuția tuturor acționarilor care aduc plus-valoare corporației; să ofere îndrumare pentru aflarea informației din mai multe perspective cheie, să suplimenteze pe viitor datele existente, să facă informația universal disponibilă și clară din punct de vedere lingvistic.

Deoarece acum există o largă audiență universală online, conceptul de BI (business intelligence), a trebuit să fie combinat, diversificat cu informații din domenii conexe, îmbrățișând concepte

vizuale pentru a reprezenta informația și a o transforma în conținut, astfel ea putând fi aplicată și comparată în mai multe domenii.

Sistemul de informații oferit de către ECM trebuie să fie acumulativ, să satisfacă toate părțile implicate și să fie universal. Din aceste motive, este necesară o atenție sporită limbajului și taxonomiei, clasificării, categorisirii informației după diferite criterii, și, de asemenea, s-a urmărit adoptarea și unor alte forme de comunicare decât doar cuvintele, cum ar fi fișierele video, diagramele sau sunetul, acestea din urmă dând naștere unor alte forme taxonomice. Instrumentele din social media ne ajută ca fiecare să poată găsi pe cineva cu care să colaboreze, informația trebuind să poată fi conectată în toate domeniile, păstrând flexibilitatea uneltelor de informare. În acest sens, comitetele aflate în organizația W3C, se ocupă de progresul acestui fenomen. Astfel, un web semantic va dizolva barierele limbii și va deschide noi posibilități de categorisire, pentru a facilita conlucrarea socială și de afaceri și colaborarea dintre organizații și participanții pieței, permițând un acces universal.

Ca urmare a prezentării de mai sus, se poate deduce faptul că, informația conținută în structurile ECM trebuie să aibă anumite proprietăți cum ar fi:

- să fie importantă pentru a fi reținută;
- să fie disponibilă atunci când este necesară extragerea ei, de oriunde ar fi necesar;
- cei care lucrează cu această informație să fie responsabili de categorisirea și conținutul ei;
- să aibă un anumit sens, pentru a fi creată, interpretată și gestionată.

De asemenea, ca o ierarhie a informației de păstrat, se poate spune că există informația individuală, apoi informația care reflectă aspecte legate de echipe, apoi de întreprindere, aceste informații care sunt apoi dezvoltate și îndreptate spre inovație.

Până la urmă, sistemul ECM depinde de trei mari factori, oameni, procese și sisteme.

Dacă ar fi să dăm un exemplu de împărțire a task-urilor în ECM și de distribuire a perioadelor de timp, se observă că, în cadrul unei întreprinderi mari, se poate ca, fiecare departament să aibă termene diferite de utilizare a informației. Ca atare, organizația poate să aibă un proces de istorie a arhivării care păstrează înregistrări foarte importante ca semnificație sau ca inovație, dar și mostre pentru vizualizare.

De exemplu, arhivele despre dezvoltare a unui produs, pot fi ținute între 3-5 ani, documentele pentru ajustări ale unui produs o lună, documente referitoare la vânzări, importante pentru calculul comisionului 3-6 luni, facturi pentru furnizori 1-3 luni, documente de garanție 1-3 ani, rapoarte corporatiste 1-2 ani. Un alt exemplu ar fi, în funcție de specificul firmei, documente medicale se păstrează pe toată durata vieții pacientului, documente de asigurări se țin de obicei pe perioadă limitată, dar uneori chiar 75 de ani, documente financiare cu anumite competențe 7 ani, etc.

Dintr-o perspectivă **economică și tehnologică**, informația unei organizații există în mod nestructurat în proporție de 70-90%, motiv pentru care ea nu este gestionată corespunzător. Acesta este un aspect foarte important, deoarece informația reprezintă proprietatea intelectuală reală a unei organizații. Informația împreună cu banii și angajații sunt cele trei elemente importante active de preț ale oricărei firme. Din acest motiv, ca un activ cheie, informația ar trebui exploatată la maxim dacă este posibil.

Pentru a colecta, stoca, înțelege, descrie, distribui și administra informația pe parcursul ciclului ei de viață, este necesară o tehnologie specifică. Pentru ca acest lucru să se realizeze într-un mod profesional, organizațiile trebuie să identifice elementele cu adevărat vitale care trebuie păstrate și să înțeleagă că acest lucru costă. Păstrarea și organizarea corectă și potrivită a informațiilor unei întreprinderi necesită un efort administrativ mare, o tehnologie de cele mai multe ori greoaie, dificil de implementat și care poate avea un efect major în cultura organizațională.

Sistemele ECM(Enterprise Content Management) oferă exploatarea eficientă a informației nestructurate, analiza de conținut în vederea identificării de tipare pentru rezolvarea de probleme complexe. Este de asemenea necesară păstrarea unui echilibru între atenția spre utilizator dar și spre automatizarea și combinarea informației structurate și nestructurate pentru luarea de decizii și inițierea de evenimente.

Această informație trebuie să fie de încredere și este necesară extragerea corectă a informației de context care să permită luarea unor decizii.

Aspectele care se iau în considerație pentru un sistem optim și profesionist de gestionare a conținutului unei organizații, sunt văzute și realizate atât din perspectiva afacerilor, cât și din perspectiva tehnică.

În cadrul companiilor mari, numărul de documente fizice și electronice este în continuă creștere, astfel încât devine tot mai greu ca aceste documente să fie găsite sau organizate într-un mod eficient. În lipsa unei bune organizări, documentele se pot pierde în email-uri, se pot rătăci prin directoarele de pe calculator sau pot fi accesate greu în arhive, dacă acestea nu sunt eficient scanate și organizate. Toate acestea pot duce la inconveniente cum ar fi încetinirea fluxului de date în cadrul organizației. Din acest motiv, **ECM** trebuie să furnizeze o soluție software de administrare și gestionare a conținutului de informații ce include aspecte cum ar fi gestiunea documentelor, fluxul de lucru, raportarea și notificările, depinzând de specificul companiilor din care acestea fac parte. Pentru organizații acest sistem reduce costurile și îmbunătățește productivitatea, permițând accesul rapid la documentație, un proces de afaceri automatizat care să răspundă în timp cât mai scurt la cererile clienților. Din punctul de vedere al utilizatorilor, este important timpul scurt și efortul minim pentru organizarea, găsirea și gestionarea de documente, prin folosirea unui motor puternic de căutare.

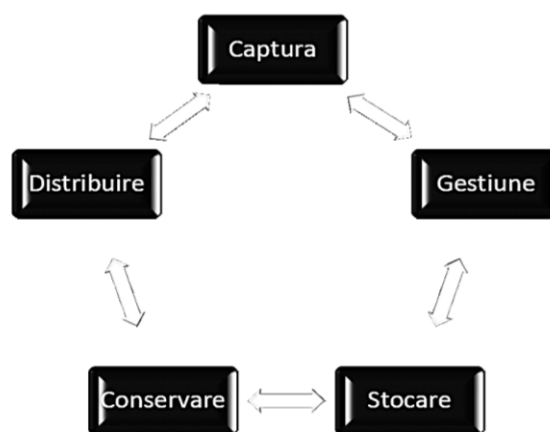
Funcțiile ECM pot fi împărțite în cinci componente majore:

CAPTURE – MANAGE – STORE – DELIVER - PRESERVE
--

- Componenta de **Captură**, care implică crearea de informație prin convertirea documentelor pe hârtie în format electronic, obținând și colectând fișierele electronice într-o structură coerentă și organizând cumva această informație. Această zonă poate include facturi, contracte, rapoarte de cercetare și multe altele
- Componenta de **Administrare/Gestiune** presupune conectarea, modificarea și întrebuințarea informației prin mijloace cum ar fi administrarea de documente, software care să permită lucrul colaborativ, în echipă, simultan asupra acelorași documente, administrarea de conținut web și de rapoarte/registre
- Componenta de **Stocare** - trebuie să păstreze pe **termen scurt** documentele cu unele copii de backup, pentru a face

față modificărilor frecvente care se realizează asupra fișierelor stocate în bazele de date, ținând cont de faptul că sunt utilizatori multipli care acționează asupra acestor fișiere și ele trebuie să poată fi vizualizate sau editate permanent

- Componenta de **Livrare/Distribuire/Furnizare** - furnizează clienților și end-user-ilor informațiile cerute
- Componenta de **Arhivare/Conservare/Păstrare** – păstrează pe **termen lung** informația care nu este modificată frecvent; această componentă se realizează de obicei prin structurile de “record management”(gestiune de registre/documente)



Sistemul ECM furnizează o platformă centralizată în care conținutul poate fi depozitat și diseminat conform unor reguli de conformitate și de securitate.

Sistemele ECM complet funcționale includ taxonomia de conținut(probleme de clasificare), furnizare de informații specifice pentru audit, integritatea datelor, minimizarea cheltuielilor, controale pentru fluxul de date cu verificare la intrare și ieșire, precum și mecanisme de securitate.

Un sistem optim de management al conținutului poate asigura un acces flux uniform și continuu de date, cu procese de business corespunzătoare acestui flux, evitându-se strangulările de informații prin reducerea înmagazinării datelor și optimizarea proceselor mecanismelor de securitate.Softul ECM trebuie să fie capabil să recunoască și să elimine duplicatele dar și să identifice excepțiile.

Cei “5C” ai ECM pot fi definiți si ca:

**CONTINUT – COLABORARE – CONFORMITATE –
CONTINUITATE – COST
(CONTENT)–(COLLABORATION)–(COMPLIANCE)–
(CONTINUITY)–(COST)**

Noțiunea de **conținut** se referă la orice conținut electronic, fișiere, date, documente, site-uri web. Include date structurate administrate într-un sistem ECM. Conținutul poate fi dinamic, adică se modifică pe parcurs, sau static, fix. Dacă conținutul merită a fi păstrat, el este transformat în fișiere și directoare. Task-ul unui ECM este acela de a captura conținutul, de a-l gestiona și de a-l face disponibil proceselor în organizație.

Colaborarea se referă la furnizarea de către ECM a informațiilor necesare, indiferent de timp sau locație. Este necesară posibilitatea de comunicare directă prin chat, forumuri, mesaje instant, conferințe video, etc. ECM trebuie să ofere informațiile exacte necesare pentru susținerea lucrului în proiecte. Colaborarea este una din cele mai mari provocări pentru lucrul eficient în organizație.

Conformitatea presupune ca informația stocată să îndeplinească cerințe legale, de arhivare securizată, cu posibilitate de urmărire a tranzacțiilor atât între organizații cât și în întreprinderea proprie. Îmbunătățirea calității și implementarea de procese eficiente sunt factorii economici importanți care trebuie avuți în vedere în proiectarea acestor sisteme, pentru ca ele să îndeplinească anumite formate standardizate (GoBS, GDPdU, Sarbanes Oxley, Basel II) pentru audit și interogare. Pentru organizație este important ca aspectul de conformitate să fie îndeplinit pentru ca investiția în aceste operațiuni să merite, să fie profitabilă.

Continuitatea în afaceri nu are încă destul credit în sistemele ECM, deși suntem tot mai mult dependenți de disponibilitatea și corectitudinea informației electronice, operațiune care este foarte costisitoare atunci când se vrea a fi profesională iar cantitatea informației este mare. ECM oferă tehnologii și metode de stocare securizată de informație cu administrare centralizată și disponibilitate distribuită, astfel ca tranzacțiile să poată fi urmărite, informația să fie protejată de orice acces neautorizat, să poată fi găsite în mod

Viitorul ECM ar fi în domeniul tehnologiilor, existând unele dezvoltări de bază și conceptuale care evoluează și modifică perspectivele ECM, astfel încât practic duc la schimbarea sistemului fundamental de gestionare a informației. Aplicațiile mobile sau cele de cloud computing sunt un asemenea exemplu, total diferite față de ce presupunea înainte păstrarea și gestionarea documentelor într-o organizație.

Social media cum ar fi Facebook de exemplu, sunt medii la fel de populare în prezent pentru comunicare, cum erau e-mailurile în anii '90. Din această zonă, pentru organizații și afaceri, devin importante metodele de comunicare, de control și de distribuție folosite aici, ele presupunând controlul complex al participanților. Mesajul organizațional devine important nu doar prin el însuși, dar și prin platforma pe care este promovat, timpul și destinatarii cărora este prezentat, toate acestea dând semnificație mesajului.

Există unelte inteligente de creare de conținut bazate pe XML, acestea permit o etichetare semantică mult mai precisă, pentru o mai bună organizare și gestionare a conținutului. ECM recunoaște conținut încapsulat, gen „snippet” de conținut. Se ajunge la liste bidimensionale, la categorisire cu cuvinte sau mapare în cloud, permițând utilizatorului lucrul dinamic cu resursele, în genul în care, de exemplu, Stephen Fry a creat cartea electronică prin care interfatarea de meta-date este folosită pentru a citi o carte neliniar, prin termeni asociați, mai degrabă decât prin citirea clasică, secvențială.

<https://searchcontentmanagement.techtarget.com>

<https://www.ecmguide.org>

<https://www.cmscritic.com>

<https://www.optimizely.com>

<https://www.makeuseof.com>

<http://stud.inf.ucv.ro/>

<https://www.todaysoftmag.ro/>

http://www.consultantaerp.ro/Servicii_ERP

<https://www.codecs.ro/business-process-management/>

<https://www.progress.com>

U Kampffmeyer: Trends in record, document and enterprise content management, Project consult Unternehmensberatung GmbH, Hamburg 2004

U Kampffmeyer: ECM Enterprise content management, Project consult Unternehmensberatung GmbH, Hamburg 2006

R Blatt: Understanding ECM industry acronyms, Electronic Image Dsigners Inc, 2009

S.Cameron: Enterprise Content Management, A business and technical guide, BCS, the chartered institute for IT, UK, 2011

Peter Rausch, Alaa Sheta, Aladdin Ayesh : Business Intelligence and Performance Management: Theory, Systems, and Industrial Applications, Springer Verlag U.K., 2013

Jv Brocke, A Simons: enterprise content management in information systems research, Springer Verlag Berlin Heidelberg, 2014

S K Shivakumar: Enterprise content and search management for building digital platforms, IEEE Press Wiley& Sons, 2017

VII. Social Media și Google Analytics

Social media = termen colectiv de site-uri și aplicații care au focus-ul pe comunicare, date generate de către comunitate, interacțiune umană, distribuire de conținut (content sharing) și colaborare.

Social media are ca scop principal interacțiunea dintre prieteni, familie și comunitate, dar din perspectiva de business, social media este folosit intens pentru marketing și promovare de produse dar și pentru studiul consumatorilor. Platformele mobile fac accesibile aspectele menționate mai sus, dintre cele mai comune făcând parte Twitter, Facebook, LinkedIn sau Instagram.

În business B2C, social media este utilă pentru promovarea brandurilor, conectarea către consumatori, crearea de noi business-uri, oferirea de feedback din partea consumatorilor, aceștia din urmă putând foarte ușor împărtăși experiența lor online, informație care ajunge rapid atât spre ceilalți consumatori dar și înspre companie.

Social media este utilă pentru ceea ce se numește crowdsourcing, adică colectarea de informații, servicii sau bunuri, companiile primind idei de la angajați sau clienți pentru îmbunătățirea produselor sau pentru dezvoltări ulterioare de produse sau servicii.

Social media poate fi utilă și în zona B2B, și anume prin analiza datelor de pe bloguri sau site-uri și folosirea acestora în luarea de decizii; prin marketing, crescând expunerea unei companii spre clienți și facilitarea accesului spre un număr de clienți mult mai mare decât prin magazinele fizice. Scopul este de a crea conținut

interesant și de impact, astfel încât clienții să îl distribuie în rețelele sociale. Componente cheie ar fi SMO-social media optimization, ca strategie de atragere de clienți noi spre website, prin adăugarea de linkuri sau butoane de share; SCRM – social customer relationship marketing – aici sunt paginile unor firme/business-uri, de exemplu cele de facebook sau grupuri de facebook sau instagram cu persoane care agreează un anumit brand și care pot afla informații despre anumite produse, clienții putând conversa între ei, furnizând astfel companiei păreri, feedback și date de marketing obținute în timp real. Astfel se pot conecta și persoane cu aceleași preocupări sau interese, în intranet intern sau rețele de colaborare, cum ar fi Yammer, Slack sau Microsoft Teams.

Prin social media, companiile câștigă foarte ușor vizibilitate, publicitatea se face în mod facil, antreprenori sau artiști pot de asemenea să devină vizibili, să creeze conținut și să efectueze tranzacții online.

Ca și dezavantaje am putea enumera dependența de internet și social media a indivizilor, polarizarea spre anumite medii, dezinformarea, postări ofensatoare, probleme de securitate sau chiar scăderea productivității unei companii prin distragerea angajaților, prea preocupați de ce se întâmplă în mediul online.

Din perspectiva companiilor, politicile în social media ar trebui să fie corecte față de clienți dar și față de companiile însele, în sensul de a nu divulga informații secrete sau stânjenitoare; strategiile ar trebui să fie cu focus înspre client, satisfacția acestuia să fie în centrul atenției, sau cel puțin așa să pară; să fie incluse imagini suficiente, sau chiar filmulețe, pentru a oferi conținut atractiv; să fie împărtășite experiențele pozitive ale clienților sau angajaților; să se urmărească instrumentele de analiză și management, gen Google Analytics.

Iată o enumerare a unora din cele mai uzuale platforme de social-media:

Facebook- utilizatorii își creează profilul, încarcă fotografii sau video-uri, trimit mesaje și păstrează contactul cu prietenii, cunoștințele sau familia

LinkedIn- este creat pentru comunitatea de business, se pot crea rețele de profesioniști pe diferite domenii

Pinterest- este un site pentru împărtășire(sharing) și categorizare de imagini găsite online, focusul este vizual; prin click pe o imagine, putem fi trimiși la sursa acestei imagini

Reddit- este un site și forum unde sunt curate și promovate “povești” – cu subiecte specifice, cum ar fi politica, muzică sau tehnologia.

Membrii trimit conținut care este apoi votat, scopul este acela de a aduce în atenție poveștile care sunt cele mai bune, cel mai bine văzute de către comunitate

Twitter- este un serviciu free de blogging

Wikipedia- este o enciclopedie open content, creată prin colaborarea membrilor unei comunități

Comunicare- utilizatorul publică conținut și încearcă să facă lumea(fans, followers) să reacționeze

Scop- generarea de reacții, de interacțiuni, de vizibilitate, creșterea vânzărilor

Conținut- sunt necesare multe postări zilnic, cu conținut de interes și de impact, pentru a stârni interesul și curiozitatea clienților (engaged audience)

Social networking = crearea și menținerea de relații în plan personal sau de business, în special în mediul online

Comunicare- este o interacțiune de vorbire și ascultare, de furnizare de informații de ambele părți

Scop- crearea unei rețele sociale din care ambele părți obțin beneficii, scopul final nefiind neapărat unul comercial

Conținut- conversații informative, întrebări, în speranța obținerii unor conexiuni sau/și a unor referințe

Statistici Facebook

FACEBOOK- a fost a doua cea mai descărcată aplicație în 2020, fiind depășită de TikTok. Urmează WhatsApp pe locul 3, Instagram pe 4, Facebook Messenger pe locul 5.

Număr de utilizatori activi lunar– update din 16 feb2022	2.91 miliarde
Nr de utilizatori telefoane mobile lunar – update din 28 iun2021	2.75 miliarde
Nr utilizatori desktop - – update din 28 iun2021; procent din totalul utilizatorilor	1.7%
	1,59 miliarde

Nr de utilizatori telefoane mobile zilnic – update din 28 iun2021	1,93 miliarde	
Număr de utilizatori activi zilnic– update din 16 feb2022		
<i>A se vedea relația cu dezvoltarea telefoanelor mobile !</i>	Nr utlizatori activi în milioane în funcție de ani	Câștigul anual FB în mилоane de dolari
2015	1591	17928
2016	1860	27638
2017	2129	40653
2018	2320	55838
2019	2498	70697
2020	2797	85965
2021*	2912	114934
În 2021 Fb a împlinit 17 ani		

Alte statistici FB

56% dintre utilizatori	Femei
44% dintre utilizatori	Bărbați
Majoritatea utilizatorilor	Între 25-35 de ani
Utilizatori din SUA	69% din populația SUA utilizează FB
Seniorii cu 65+	4.8% din utilizatori
23.8% utilizatori	Între 18-24 de ani
90% din utilizatorii FB	Din afara SUA și Canada
320 milioane utilizatori	Din India –cei mai numeroși utilizatori ai unei țări
190 milioane utilizatori	SUA –locul 2, după India
Peste 10 milioane	Cei care își fac publicitate pe FB
În 2020 venitul pe reclame	27,187 milioane dolari

În 2021 venitul pe reclame	32,639 milioane dolari
75% din Fb users vizitează cel puțin un business local	O dată pe săptămână
1.72 dolari	Este costul mediu cost per click CPC

În prezent, un rol important în dezvoltarea marketingului online îl ocupă activitatea efectivă a consumatorilor și postările acestora, fiind dominat de influenceri, review-uri și păreri ale utilizatorilor, precum și alte tipuri de postări de conținut online. Cu ajutorul inteligenței artificiale și a analizei big data, se realizează strategii noi de reclamă și de oferte de produs pe platforme cum ar fi Instagram, TikTok, Twitter, Facebook sau Youtube. Influencerii și relațiile virtuale sociale, care creează cel puțin virtual, loialitate față de brand, reprezintă astăzi factori deosebit de importanți în comportamentul consumatorilor, în impactul cumpărăturilor din mediul online. Implicarea consumatorilor este determinată de conținutul imersiv și de evoluția platformelor. Pentru a observa mai bine comportamentul consumatorilor, pentru a se sublinia autenticitatea produselor și calitatea conținutului, prelucrarea de date referitoare la consumatorul din mediul online este vitală. Aceasta asigură definirea unor strategii practice pentru specialiști și cercetători, ca urmare, oferind clienților conținut personalizat cu rezonanțe emoționale specifice. Platformele social media nu doar au audiențe foarte largi dar și angajarea directă a firmelor cu clienții.

În 2025 regula de social marketing care funcționează cel mai bine este cea de 50 30 20, adică 20% din postări sunt de tip promoțional, 30% specifice de brand iar 50% din postările de conținut să evidențieze valoarea produselor.

Câteva direcții specifice și care ar trebui respectate în planul de marketing digital care include aspectele legate de social media:

- Planificare și strategie, creând targeturi clare cum ar fi awareness de brand sau grupe specifice de clienți; acestea se stabilesc foarte clar în platformele de Google Ads de exemplu, create exact în aceste scopuri și care dau rezultate foarte bune
- Crearea de conținut ce conține imagini, video, stories, pentru atenție
- Administrarea platformei prin optimizarea de profiluri și folosirea unui branding cu consistență

- Crearea unei comunități prin permiterea utilizatorilor să comunice, să facă review-uri, să transmită mesaje și să creeze loialitate
- Analitici pentru măsurarea diversilor parametri de succes, de conversie, de vizualizare a caracteristicilor profilurilor utilizatorilor
- Reclama personalizată depinde de vârstă, locație, alte detalii demografice și arii de interes
- Marketing de influenceri este realizat prin parteneriate cu diferite personalități de impact pentru o anumită zonă de clienți
- Comunicare bidirecțională dintre firme, organizații și clienți
- Este de asemenea de studiat, în funcție de produsele promovate și audiență, care dintre platforme potrivește mai bine

Trenduri de e-commerce în 2023

Focusul pe valoare, ca urmare a recesiunii globale. Pe scară globală, există incertitudinea politică și criza costurilor ridicate care impactează clienții, obiceiurile acestora de a cheltui, lanțurile de aprovizionare și costurile operaționale din business. Astfel încât, pentru a convinge clientul să cumpere, în moment de criză, când și prețurile au crescut, este necesară o experiență excepțională însoțită de un client service deosebit. De asemenea trebuie avute în vedere aspecte ca returnări simple de marfă prin politici prietenoase, reducerea materialelor printate, evitarea sau reducerea costurilor de transport, programe de loialitate. Comunicarea cu clienții trebuie realizată pe canale preferate de aceștia.

Consumatorii trebuie încurajați să aleagă **produse sustenabile** mai degrabă decât să cumpere în grabă, produse de proastă calitate. Încă nu este o prioritate sustenabilitatea, doar 8% din clienți sunt de-adevăratelea preocupați de aceste aspecte, restul sunt mai interesați de procesul de cumpărare și de produsele achiziționate. Totuși există organizații europene care insistă pe opțiuni eco de transport și ambalare pentru modificarea comportamentului consumatorilor în timp.

O experiență deosebită cu acel brand. Este necesară o viziune de prezentare a brandului care să evidențieze calitatea brandului și experiența pe care acesta o furnizează consumatorului. În prezent, din cauza protecției datelor, Google furnizează mai puține informații decât în trecut, astfel încât platforma, conținutul, SEO, activitățile de live-streaming sau conținutul video, trebuie să asigure, pe lângă calitatea de excepție, o experiență afectivă pozitivă pentru consumator. Brandul trebuie să fie transparent, autentic, abordabil, deschis unei largi audiențe. Este importantă existența de video-uri sau fotografii online în care userii testează, probează produsele, le prezintă ca fiind valide, conform descrierii, reclamei și funcționalității acestora.

Design elegant al site-ului. În trend pentru 2023 este un design aerisit, cu spațiu suficient între câmpurile vizuale, astfel încât focusul să cadă pe imagini, pe produs. Nu este de dorit ca site-ul să fie aglomerat. Se pune accentul pe grafica custom, pe artă personalizată care redă specificul produselor acelui site. Este important ca site-ul să reflecte personalitatea și unicitatea brandului. Cursori animate, scrolling și un styling asimetric sunt trenduri pentru 2023.

Focus pe online marketing. Se prevede creșterea bugetului pentru reclame pe diferite platforme, unii preferând Facebook sau Google, dar alții căutând platforme mai mici dar mai nișate, corespunzătoare cu produsele pe care le oferă. Criza va crește nevoia de competitivitate a brandurilor. Marketingul targetat este și rămâne important prin SEO (search engine optimization) și SEA (search engine advertising), ambele fiind specifice pentru Google și sunt instrumente strategice pentru ca brandurile să rămână în top, să aibă vânzări și succes pe termen lung.

Live shopping. Acest tip de shopping care exista înainte ca și emisiuni TV, acum în mediul online este mult mai accesibil, mai impulsiv, promovat de social media. Poți influența audiența pentru accelerarea vânzărilor și deciziilor, creșterea angajamentului consumatorilor și a experienței prin demo-uri. Unele branduri obțin astfel o creștere a vânzarilor de 30%. Este un instrument foarte util de prezentare pe platforme gen TikTok sau Amazon Live a unor oferte extraordinare din toate domeniile.

Conținut video în formă scurtă. Unele site-uri au tendința să dea o impresie de "TikTok" prin prisma videourilor care prezintă marfa sau ofertele. Multe aplicații conțin posibilitatea ca site-uri de vânzări să aibă conținute elemente de tip "Stories". Reels pe Instagram,

filmulețe de tip TikTok sau Youtube Shorts prezintă filmulețe prietenoase, ușor de “digerat” pentru consumatori. Brandurile se pot folosi de acestea pentru creșterea audienței și pentru ca clienții să conștientizeze existența brandului. Pentru proprietarii de business-uri mici, sunt utile video-urile educaționale pentru a-și demonstra cunoștințele, a-și prezenta produsele sau a arăta cum aceste produse trebuie folosite. Deoarece aceste filmulețe sunt limitate la câteva secunde sau minute, ele trebuie să fie destul de concise și la obiect.

Folosirea IA și a realității virtuale. Este foarte importantă deoarece este oarecum similară cu experiența pe care utilizatorul o poate avea în magazinul fizic, permițând ca acesta să probeze produsele, cum ar fi de exemplu haine sau produse de machiaj. Sau, mai mult, există haine virtuale care se pot cumpăra, ele neexistând în viața reală. Acest tip de tehnologie permite pentru cumpărător o experiență satisfăcătoare și unică, dar deschide și posibilitatea ca producătorii să prezinte produsele înainte ca acestea să fie realizate fizic, produse efectiv. Clientul poate totodată să aleagă în realitatea virtuală varianta preferată pentru ca aceasta să fie executată pentru el. Acest lucru personalizează experiența clientului.

Ce înseamnă marketing-ul digital în 2023?

Pe întreg globul sunt cca 1.5miliarde de utilizatori social media. În primul rând, utilizatorii trebuie să simtă că au control asupra datelor lor. Dacă acest control le lipsește, ei devin sceptici. Utilizatorii trebuie să aibă acces permanent la instrumente pe care să le înțeleagă și folosească ușor pentru administrarea aspectelor de protecția datelor proprii.

Conform studiilor, cca 20% din afacerile existente pe piața online, își vor crește bugetul alocat marketingului cu 50%. De asemenea se va pune accent pe conținut creat prin IA- inteligență artificială. Se presupune că strategiile de marketing vor fi conduse de algoritmi IA.

Se pare că în zona online, comerțul digital va avea succes deoarece există foarte mulți consumatori conștienți de mărfurile și informațiile existente pe piața digitală. Cei care se ocupă de business au la dispoziție o gamă largă de instrumente smart pentru colectarea datelor și pentru a realiza analize esențiale despre audiența lor(target audience). Aproximativ 77% din companiile din întreaga lume au adoptat strategii potrivite de marketing digital pentru a-și asigura un loc pe piața online.

Ca și joburi de top potrivite pentru aceste aspecte referitoare la comerțul digital, ar fi:

- Dezvoltatori Cloud computing, aici intrând atât aspecte legate de arhitectură, programare propriu-zisă dar și gestionarea bazelor de date
- Inteligență artificială și machine learning (AI+ML)
- Marketingul digital și strategiile acestuia
- Știința analizei Big Data (datelor virtuale structurate și nestructurate existente în mediul online și disponibile în urma analizelor și statisticilor) referitoare la tipare ascunse, corelații, trenduri de piață și preferințe ale utilizatorilor

Trenduri social media și influenceri

TikTok a devenit un element important în social media, deoarece a generat sume ca 4.6 miliarde dolari în 2021, o creștere de 142% în 2022 datorate a 1.8 miliarde de utilizatori activi în 2022. Platforma se axează pe utilizarea ei pentru business și îmbunătățirea tehnicilor de targetare ale reclamelor, prin instrumentul “ads manager targeting”. În social media utilizatorii fac cheltuieli de aproximativ 33% din veniturile lor din mediul digital, conform Wordstream.

Se prevede descentralizarea social media, astfel încât utilizatorii migrează de la o aplicație la alta. Twitter a pierdut teren, dar Mastodon, creat de masele de utilizatori, devine interesant prin numărul enorm de descărcări care se face zilnic de pe platformă. BlueSky este mai mult o infrastructură decât o platformă, se dorește o nouă fundație pentru social networking, astfel încât participanții devin independenți de platforme, dezvoltatori și își pot crea singuri experiența proprie.

Brandurile sunt nevoite să creeze conținut care să atragă clienții într-o perioadă de criză, dominată de lipsuri și foame. Sunt importanți creatorii de conținut și influencer-ii. Social media nu se mai focusează pe numărul de urmăritori ci pe crearea unui conținut de valoare.

30% din utilizatorii între 18-24 de ani, și 40% dintre utilizatorii între 25-34 de ani se consideră creatori de conținut.

În prezent reclamele video ocupă un loc important, 86% din companii folosesc video-ul ca și instrument de marketing iar 92% din firme îl consideră ca o parte foarte importantă de strategie. Aceste video-uri

sunt în special pe Youtube, LinkedIn și Instagram. Conform digitalmarketinginstitute.com

Scopul creării fimulețelor	%
Explicative	74
De Social media	68
De prezentare	50
Testimoniale	46
Reclame	42
De vânzări	41
De produs	40
De reclamă teaser	37
De către clienți	29
Grafică video	26
Pentru explicare la customer service	21
De customer service	20
Demo de aplicații	15
De angajare	12

Conținutul creat pe social media poate însă avea scopuri diverse, fie creșterea vânzărilor, sau apropierea față de clienți, informarea acestora, crearea de conversații pentru a afla părerile clienților, creșterea încrederii clienților față de firmă și produsele acesteia.

78% dintre companii au o abordare strategică pentru administrarea de conținut, doar jumătate dintre aceștia au o strategie documentată care studiază atent datele despre consumatori legate despre modul în care aceștia percep de exemplu valoarea și etica brandului. Aceasta deoarece un element important pentru vânzări devine comunitatea; oamenii caută comunitățile, grupurile, caută firme ale căror valori sunt similare cu valorile proprii. Astfel, în ochii clienților, un brand apreciat este acela care ține cont de influenceri, de conținutul generat de către utilizatori; un brand care devine cunoscut prin vocea clienților nu prin vocea proprie, **CHIAR DACĂ BRANDURILE AU CONȚINUT PROPRIU ȘI VOCE PROPRIE** (în esență). Deci ar trebui făcut un echilibru între cele două.

Pentru firme mici și lansări de produse, email-urile sunt de departe cele mai eficiente și sunt folosite de 89% din organizații. Aproape toată lumea are un email, atfel încât conexiunea firmelor cu clienții este facilă. Se au în vedere atât clienți care au cumpărat deja

produse de la firma respectivă dar și cei care sau înscris în baza de date și încă nu au cumpărat. Se pune însă accent pe creativitate în atragerea clienților, cum ar fi de exemplu prin survey Moneky. Totuși în momentul în care cineva se decide să folosească o platformă, este bine să găsească varianta cea mai potrivită atât ca instrument cât și ca și cost pentru afacerea respectivă.

În 2023 se dorește anticiparea dorințelor clienților, personalizarea dorințelor și furnizarea lor prin platforme ca și Google Ads+Facebook (de exemplu). Este important comportamentul utilizatorilor pentru că reflectă interesele acestora, dar și “semnale” prin care clienții ne transmit ceea ce ei ar dori. Astfel se prevede ca în 2024, organizațiile cu echipe de IT care se ocupă de înțelegerea și previziunea nevoilor clienților să depășească cu cca 20% performanțele firmelor care se ocupă de statistici și studiul metricilor. Astfel se dorește automatizarea și personalizarea instrumentelor pentru CRM, social media, reclamă, management sau email. Automatizare, în cazul acesta ar însemna culegerea de date, stocarea lor într-o unealtă care de fapt să realizeze automatizarea comunicării cu clienții, cum ar fi de exemplu prevederea următoarelor acțiuni pe care utilizatorul le va întreprinde, bazat pe comportamentul său din trecut.

GPT-4 Generative Pre-trained Transformer este un model deep learning, de învățare artificială bazat pe datele disponibile pe internet. Este folosit pentru întrebări și răspunsuri, texte, traduceri, clasificări, generare de cod și conversații.

Înainte de GPT era folosit modelul NLP –natural language processing, antrenat pentru clasificări sau traduceri. Acesta se baza pe învățarea supervizată, care avea anumite lipsuri cum ar fi absența unor date notate(notițe) și greșeli la operații de generalizare.

GPT1= Improving Language Understanding by Generative Pre-Training

GPT1 a apărut în 2018 propunând un limbaj generativ antrenat pe date neetichetate și realizând operații de finețe pe clasificare și analiza de sentimente. Parametrii erau de 117M.

GPT2= Language Models are Unsupervised Multitask Learners, apare în 2019, antrenat pe seturi de date mai mari având mai mulți parametri, creând un model mai puternic. Parametrilor li se alocă dimensiunea de 1.5B, iar pentru condiționarea atribuțiilor(taskurilor) se folosesc învățarea zero-shot.

GPT3= Language Models are Few-Shot Learners(2020), parametrii sunt de 175B, modelul are de 100 de ori mai mulți parametri decât varianta GPT2, setul de date de antrenare este și el mai mare pentru

obținerea de rezultate bune. Pentru condiționarea atribuțiilor(taskurilor) se folosesc învățarea cu setări zero-shot, one-shot și few-shot, folosind învățarea în context, în funcție de context. A surprins prin acțiuni cum ar fi scrierea “creativă” asemănătoare celei umane, scripturi în Python, traduceri și rezumate-sinteze.

Se așteaptă în prezent GTP4, cu parametri până la 280B, unde se precizează că dimensiunea mai mare a parametrilor nu înseamnă performanțe mai bune. Se dorește obținerea de modele mai mici cu performanțe mai mari, ceea ce va rezulta în seturi mari de date, masive resurse computaționale și implementare complexă. Va fi focusat în special pe operațiuni gen text-to-image sau recunoaștere de vorbire (speech-recognition).

Trenduri de E-Commerce în 2024-2025

Comerț în social media	Vânzări prin intermediul platformelor de social media care se estimează a se tripla până în 2025, ajungând la 1200 de miliarde de dolari. Se mizează pe platforme built-in: Tiktok Shop, Instagram Shopping, Shops pe Facebook, reclame Pinterest “cumpărabile”. Traficul pe mobil reprezintă 80% din traficul pe social media. Facebook este cea mai populară platformă în lume cu 2.9 milioane de utilizatori.
Personalizare cu AI	Bazat pe inteligența computațională și “Big Data”,

	firmele pot antrena AI pentru a-și adapta afacerea la comportamentul consumatorului. Prin personalizare se croiește profilul de vânzare pe baza informațiilor existente despre client. Conform studiilor, 80% din clienți revin în urma acestor oferte personalizate. Exemplu Starbucks care are atât oferte și mesaje personalizate dar și scrierea numelui pe pahar.
Mobile shopping	Site-urile trebuie să fie mobile-friendly deoarece marea majoritate a clienților (cca 62% - 70% în 2024 marketer.com) cumpără online.
Firme sustenabile	“Politici verzi”, sustenabilitate sunt caracteristici pe care clienții le susțin deoarece se aliniază la credințele lor. 80% dintre aceștia iau în considerare și aspectul ecologic atunci când aleg să cumpere online. Multe din problemele actuale au ca și cauză prioritizarea profitului în

	defavoarea moralității sau a aspectelor ecologice. De aceea este cel mai bine ca orice afacere să se concentreze și pe direcții care țin de ecologie. 65% dintre consumatori urmăresc să cumpere produse ambalate eco-friendly, 29% evită ambalajul care conține plastic, 64% dintre consumatorii US și UK cer ca firmele producătoare de îmbrăcăminte să folosească mai puține ambalaje.
Chatbots	Bazați pe AI, urmăresc să învețe repede din comportamentul clientului cum să interacționeze cu acesta. De asemenea oferă răspuns imediat și dau și sugestii de cumpărături iar multora dintre clienți li se pare important să fie tratați ca și cum toată atenția este concentrată doar pe persoana lor.
Voice search – Căutare vocală	Căutarea vocală pe internet oferă oamenilor posibilitatea de multitasking, de a realiza simultan mai multe acțiuni. 47%

	dintre consumatori folosesc această proprietate pentru cumpărături online, în special cele de strictă necesitate, iar 58% dintre aceștia au fost chiar mulțumiți. Se estimează un salt de la 11 miliarde de dolari cheltuiți astfel în 2022 la aproape 50 miliarde de dolari în 2029. Ca și întrebări, lumea are tendința de a interoga, în special pe Google, întrebări clare, nu cuvinte cheie și nu fraze întregi.
Modele de abonamente	Important abonamentul pentru că astfel cresc șansele pentru ca clienții să revină. Din studii reiese faptul că e mai ușor să păstrezi clienții existenți decât să aduci alții noi. Abonamentul oferă clienților în mod recurent experiența pozitivă a cumpărăturilor online. Exemplu: Hello Fresh prin kituri de mancare zilnică a atras cca 7 milioane de consumatori
Realitate virtuală și augmentată AR și VR	Se așteaptă să crească în 10 ani cu 40% și să aibă profit de cca

	850 miliarde de dolari în 2031. Tehnologiile AR și VR oferă o experiență imersivă mai intensă, prin simularea acesteia folosind sunet, imagini vizuale și alți stimuli. Conform studiilor, 71% dintre clienți ar cumpăra mai mult dacă ar putea avea experiența AR. IKEA folosește platforma Apple ARKit care permite clienților să vadă cum arată obiectul din magazin într-o simulare 3D la ei acasă sau în orice alt spațiu.
Livrare rapidă	
Influencer marketing	Consumatorii nu au întotdeauna încredere în publicitatea tradițională, dar au încredere în recomandările altora. Crește traficul organic și atrage noi clienți cu costuri mici. Statistic, pentru fiecare dolar investit, se generează în medie un profit de 5.78 dolari. Metodă eficientă pentru 60% din vânzătorii online, pentru care profitul generat prin influenceri

	este mai mare decât prin postări ale unui anumit brand. 80% din consumatori cumpără un produs pentru că este recomandat de către influenceri. Ex Net-a-porter recomandată de actrița Shilene Woods
Modalități flexibile de plată	În afară de carduri de credit sau debit, transferuri bancare, plata ramburs la primirea coletului, se preferă modul de plată prin dispozitivul mobil, portofelul digital (49% în 2021), Google Pay, alte aplicații mobile sau chiar criptomonede. Preferințele oricum diferă în funcție de țară sau regiune.
Exemple:	
Coreea de sud	6% transfer bancar 16% ramburs 22% portofel digital 56% carte credit
Tailanda	12% carte de credit 23% portofel digital 28% alte plăți, ramburs 37% transfer bancar

Cele mai apreciate Platforme de social media	%
Instagram	28.19
Youtube	27.04
TikTok	23.94
Facebook	9.85
LinkedIn	8.59
Twitter	2.39
Video – tipul de conținut video care a generat cele mai multe reacții	%
Videouri scurte	31.38
Video în format lung	15.51
Podcasturi, Expert talks	13.84
Video cu tema romantică	12.37
Memes	10.31
Conținut generat de utilizatori	10.12

Altele	6.47
Conținut bazat pe text *Conținutul să fie mai mult ca o conversație Să includă ambele părți, să conțină și cuvântul “Tu” Să păstreze treaz interesul clientului de exemplu prin întrebări Ideile să fie scurte și la obiect Să ofere informații interesante	%
How to	38.53
Listicles = conținut text prezentat ca listă, are un titlu care specifică numărul de elemente conținute în text, putând avea și subtitluri pentru textele de la fiecare intrare-paragraf. Listicle = list+article	32.71
Evenimente curente	7.49
Rapoarte de studiu	5.02
Interviuri	3.97

Stories	2.38
Altele	9.0
Profit pe Social Media	%
X	6.8
Pinterest	5.2
Snap	4.9
TikTok	4.1
YouTube	3.9
Instagram	3.3
Facebook	3.2
LinkedIn	2.6

De ce clienții abandonează coșul de cumpături?

Motiv	%
Costuri extra prea mari, precum taxa de transport, vama etc	48
Este necesară crearea unui cont	24
Livrarea a durat prea mult	22
Neîncrederea în transmiterea datelor de card pt acel site	18
Procesul de checkout era prea complicat și dura prea mult	17

Nu se putea vedea de la început costul total, final	16
Website-ul s-a blocat	13
Nemulțumiri în ce privește politica de retur	12
Insuficiența modalităților de plată	9
Cardul de credit nu a fost acceptat	4

Google Analytics

Este un instrument foarte important pentru monitorizarea traficului web, pentru urmărirea obiectivă, colectarea de date și informații, măsurarea și analiza datelor din mediul online în vederea obținerii de situații și strategii de marketing. GA permite observarea modului în care utilizatorii navighează și se comportă în mediul online și cum aceste criterii depind de diverși parametri cum ar fi vârsta sau alte date demografice. Pentru a folosi acest instrument, este necesar a avea un cont de Google.

Se adresează în primul rând designerilor și dezvoltatorilor de produse web, celor care produc conținut online precum și proprietarilor de pagini web

GA este un software free care monitorizează utilizarea și utilitatea unei pagini web, în ce privește designul și conținutul acesteia.

GA studiază datele de pe internet în ce privește colectarea, măsurarea de obiective, realizarea de analize, pentru optimizarea paginilor web și a studiilor de marketing. Altfel spus, acest instrument ajută la înțelegerea modului în care utilizatorii folosesc pagina web și la îmbunătățirea acestui aspect.

Este un program util în special pentru proprietarii de afaceri mici (small business) și pentru organizațiile non-profit. Ca și competitor pentru GA ar fi de exemplu Yahoo Analytics.

GA se setează printr-un cont Google pentru a urmări modul în care utilizatorii navighează pe un site și modul în care aceștia vizitează alte site-uri sau linkuri (adică unde și pe ce dau click)

GA poate fi ușor de implementat și furnizează o cantitate impresionantă de date, este facil chiar și pentru cei care nu au multe cunoștințe de programare.

Secțiunea de rapoarte este organizată ca o pagină web sau un dashboard cu widget-uri personalizabile care se pot adapta nevoilor individuale.

Proprietăți:

Audiența – aceste rapoarte arată din ce orașe provine traficul și ce tehnologie este utilizată pentru navigare, acest din urmă aspect este important pentru stabilirea designului paginii web, spre a fi mai ușor accesibilă și de vizualizat de pe telefon, calculator, tabletă, etc.

Sursele de trafic – aceste rapoarte sunt utile pentru a înțelege cum au ajuns utilizatorii la site-ul în studiu, ce cuvinte cheie au folosit pentru căutare, care i-a adus la pagina respectivă. Raportul “keyword” din cadrul opțiunilor de căutare este foarte important pentru a înțelege intenția utilizatorului care a ajuns pe pagina în discuție; adică au căutat pagini referitoare la un cuvânt cheie sau încercau să ajungă chiar la pagina asupra căreia se face studiul.

Conținut – acest aspect include un raport referitor la sortarea paginilor vizitate, evidențiindu-se site-urile cele mai ~ sau cele mai puțin vizitate. La partea de raport legat de conținut, se specifică și timpul de încărcare al paginii.

Scopuri urmărite – acest aspect este corelat cu aplicații de e-comerț și tranzacții care să permită achiziționarea unui produs în urma vizitării site-ului. Aici sunt incluse și campaniile legate de social media.

În ce privește **ierarhia** în cadrul GA:

Organizații: conțin produsele și utilizatorii; organizația este de fapt compania care oferă acces la conturile de produs ale companiei. Se pot face integrări între produse și permisiunile utilizatorilor pentru aceste produse.

Conturi: ele oferă accesul la GA; se pot conecta mai multe asemenea conturi la o aceeași organizație

Proprietăți: reprezintă o aplicație sau un site, un cont putând conține una sau mai multe proprietăți. Când se culeg date dintr-o aplicație, o proprietate ar trebui să fie conectată la o singură aplicație, de exemplu cea de mail gmail.

Fluxul de date: arată fluxul de date care se transferă de la client spre GA. Se pot adăuga mai multe asemenea fluxuri, cum ar fi cele provenind de la o aplicație Android, alta de la iOS iar altul de la o pagina web. Se pot vizualiza toate datele din diferite fluxuri în raport sau se poate realiza filtrare doar pe fluxuri dorite.

Organizație	Conturi ->	Proprietăți ->	Flux de date
			Flux de date
			Flux de date

Păstrarea datelor: se poate seta durata pentru care aceste date să fie păstrate; ele pot fi referitoare fie la utilizatori fie la diferite evenimente.

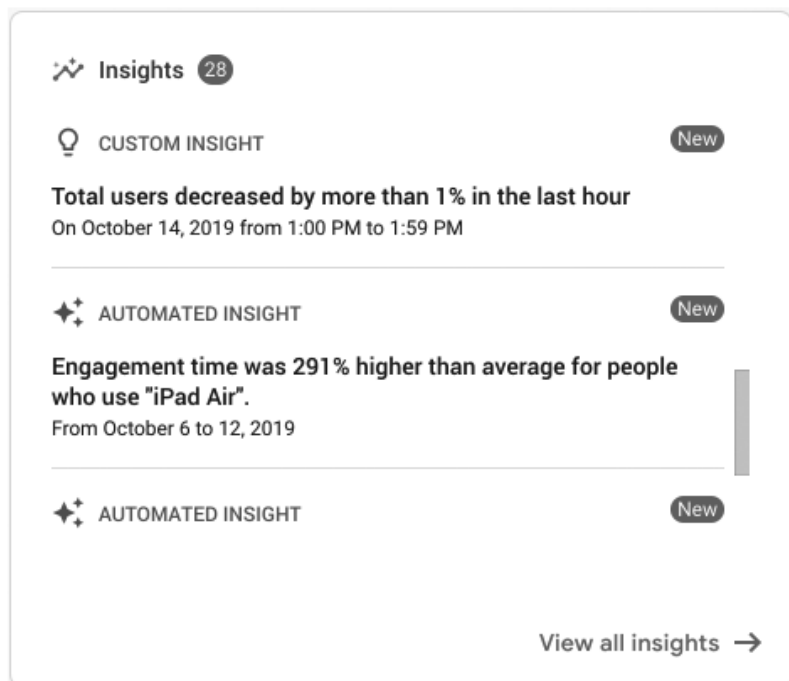
Evenimente: acestea dacă sunt colectate automat, se fac prin interacțiuni de bază ale utilizatorilor cu aplicația sau site-ul, datele despre evenimente apărând vizibile în rapoartele GA. Pentru fiecare eveniment se colectează date implicite cum ar fi limba, locația paginii, referința la pagină, titlul acesteia precum și rezoluția ecranului. Numele evenimentelor care colectează datele sunt sugestive pentru acțiunile pe care acestea le realizează, și anume **ad_click**(userul dă click pe un anunț), **ad_exposure**(când pe ecran apare cel puțin un anunț difuzat de SDK pentru anunțuri mobile), **ad_impression**(utilizatorul vede o afișare a anunțului), **ad_reward**(acordare de recompensă pentru anunțuri mobile), **clic**(userul dă click pe un link de părăsire a domeniului în studiu), **file_download**(utilizatorul apasă un link care duce la un fișier care poate avea extensie de tip doc, txt, exe, ppt, mp3, ...) etc.

În ce privește **evenimentele** specific **comerțului electronic**, acestea pot fi de anumite tipuri specifice, cum ar fi: **add_payment_info**(utilizatorul trimite informații de plată), **add_shipping_info**(utilizatorul adaugă informațiile pentru expediere), **add_to_cart**(adăugare în coș), **add_to_whishlist**(adăugare în lista de dorințe), **select_item**(produs selectat dintr-o listă), **view_item**(utilizatorul inspectează un produs) etc

Statisticile care sunt oferite, sunt de fapt un set de funcții cu proprietate de învățare automată și condiții/setări care se configurează pentru obținerea unor date utile. GA oferă două tipuri de statistici:

Statistici automatizate, unde sunt detectate modificări neobișnuite sau tendințe ale datelor, informarea făcându-se automat în raportul de statistici din cadrul platformei GA

Statistici personalizate, care permit crearea unor condiții customizate pentru detectarea de modificări importante de date; se pot primi și alerte e-mail. Pentru fiecare proprietate se permite crearea de maximum 50 de statistici.



Instrumentul de **analiză** permite gruparea de date în ceea ce se numește în GA hub-ul de analiză, acesta conținând toate analizele create sau trimise. Analiza constă din mai multe date care se pot consulta prin tehnicile de analiză. Tehnica arată modul de studiu al datelor conținute în fișe, și anume se pot face analize folosind tehnicile următoare:

Explorare: datele sunt afișate putându-se opta pentru diferite tipuri de explorare și vizualizare, cum ar fi grafice cu bare, diagrame radiale, cu linii, cu puncte sau hărți geografice.

Analiza de canale: prezintă calea utilizatorilor parcursă de aceștia în descoperirea site-ului, fiind utilă pentru identificarea zonelor cu performanțe extreme, adică foarte bune sau foarte proaste. Se observă astfel dacă utilizatorii reușesc sau eșuează în parcursul lor prin site. Astfel se pot reduce căile ineficiente sau cele abandonate de către clienți.

Suprapunerea de segmente: conține analize cu diagrame Venn, arătând interecția intereselor utilizatorilor după anumite criterii.

Exploratorul de utilizatori: definește și prezintă segmentele de utilizatori, aici se pot consulta individual activitățile acestora în parte.

Analiza căilor: arată experiența utilizatorilor prezentată într-o anumită ierarhie, având astfel acces la modul în care utilizatorii interacționează cu site-ul și cu aplicația.

Variabilele care apar în aceste analize sunt date ca set de parametri, valori și segmente folosite de GA pentru analiză.

Setările sunt variabile folosite în concordanță cu tehnica de analiză aleasă, ele incluzând filtre și alte opțiuni pentru tehnica curentă folosită.

Se pot crea maxim 200 de analize individuale per utilizator pentru fiecare proprietate și max 500 de analize comune pentru fiecare proprietate și se pot importa max 10 segmente pentru fiecare analiză.

Un **segment** este un subset de date colectate prin GA care prezintă o anumită proprietate, de exemplu dintr-o mulțime de utilizatori, un segment pot fi cei care sunt dintr-un anumit oraș sau cei care se încadrează într-o anumită grupă de vârstă, cei care cumpără un anumit tip de produse sau care vizitează o anumită secțiune specifică a site-ului. Un exemplu util de prelucrare a acestor date ar fi dacă de exemplu se observă că utilizatorii dintr-un anumit segment, nu mai achiziționează produse de un anumit tip, atunci trebuie observat dacă a apărut o companie concurentă care produce același lucru la preț mai mic, caz în care de exemplu se pot face reduceri de loialitate.

Segmentele se pot structura pe mulțimi de utilizatori cu un comportament similar, mulțimi de sesiuni care se referă la o anumită activitate specifică (cumpărare în cadrul aceleiași campanii) sau segment de accesări, la care toate accesările sunt cu anumite proprietăți indicate pentru studiu. Se pot folosi max 4 segmente în cadrul aceluiași raport.

Explorarea datelor obținute din rapoarte se poate face prin afișarea lor în tabele, unde rândurile și coloanele se pot organiza customizat, se pot grupa datele și se pot aplica segmente și filtre. De asemenea datele se pot vizualiza și sub formă de grafice.

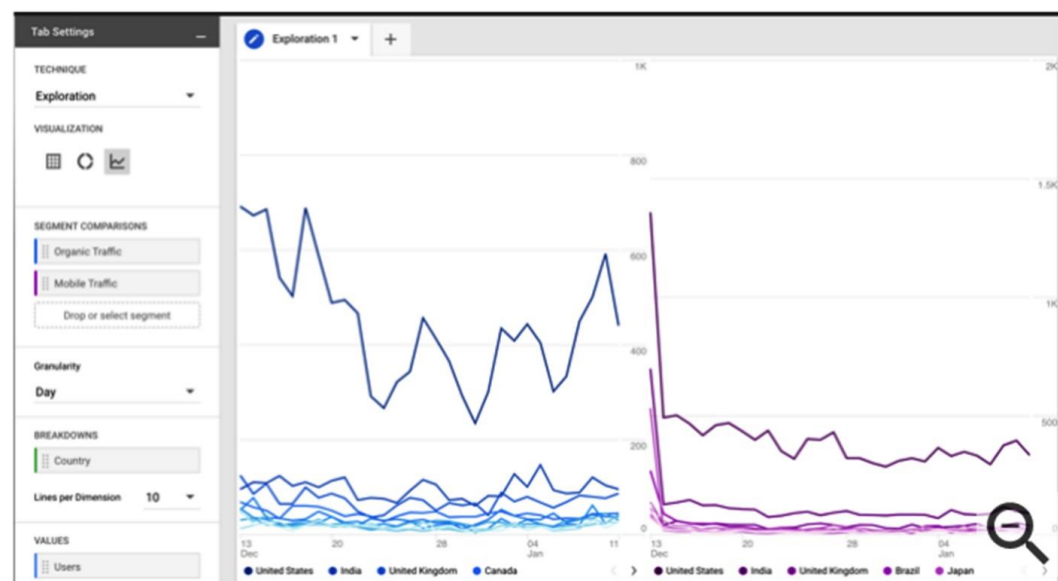
Exploration 1 +

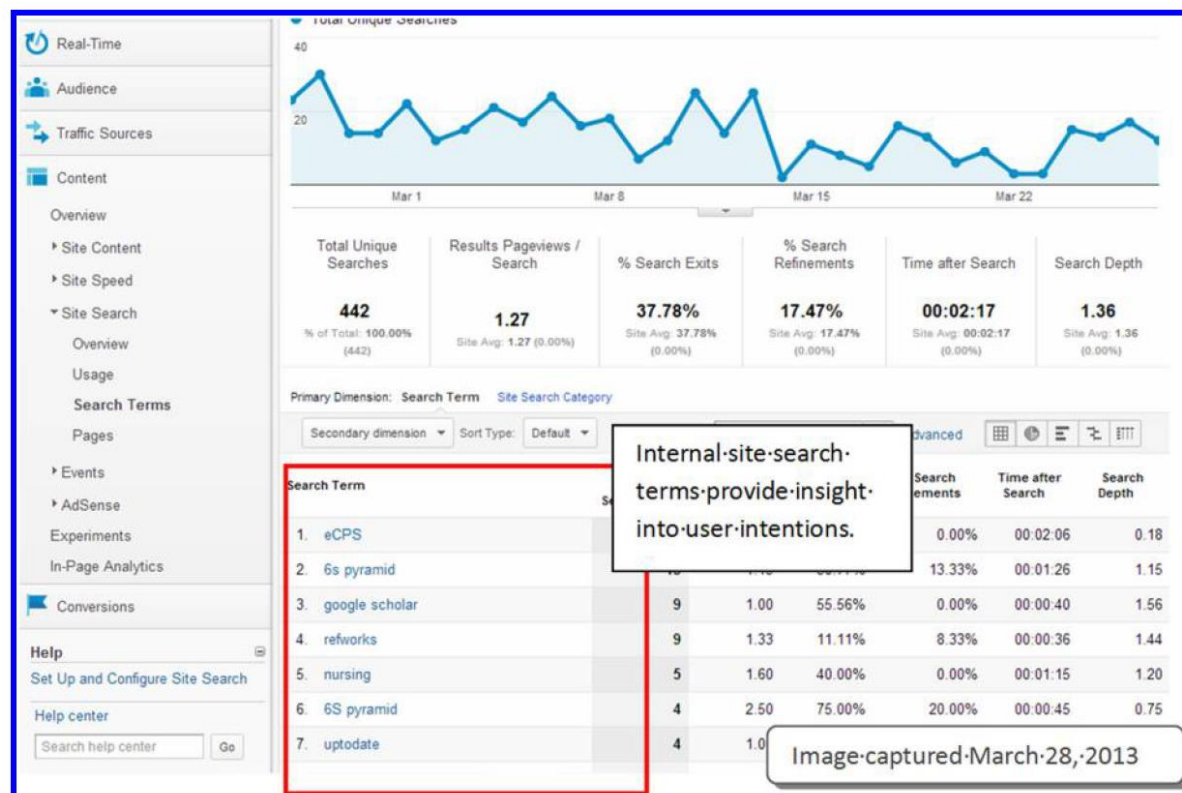
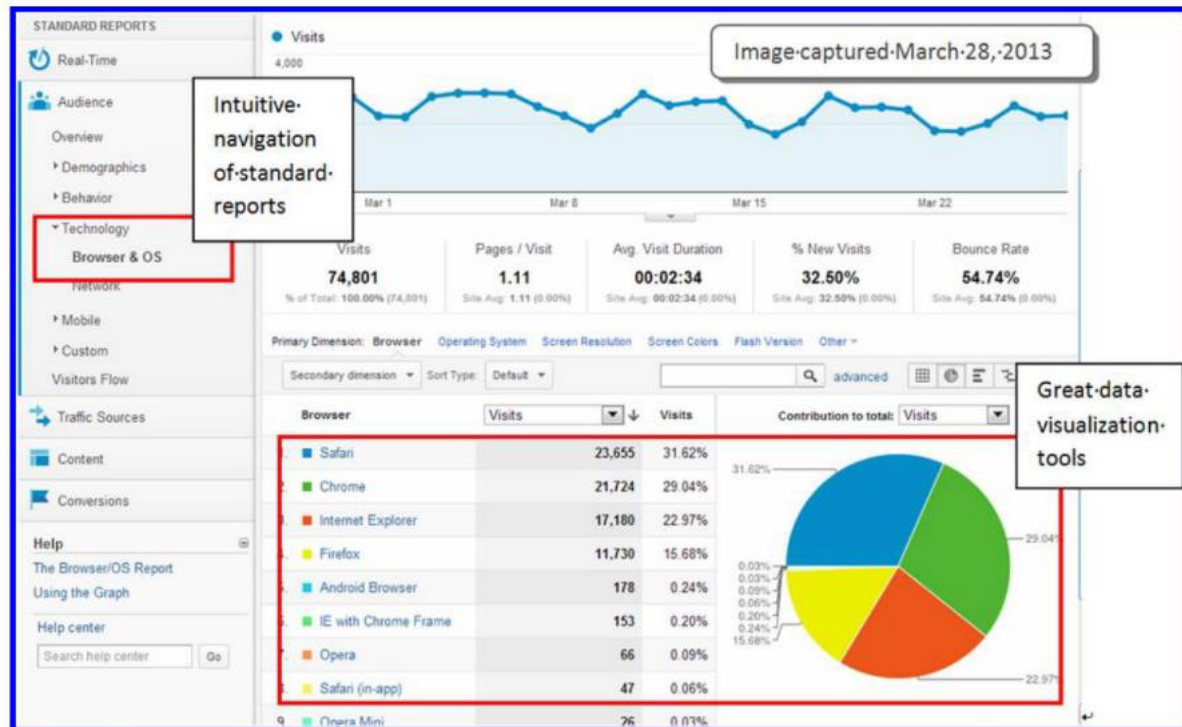
Device Cate... desktop

Screen Resol... 360x540 1366x768 1440x900 1920x1080 375x667

Country	Users	Revenue	Users	Revenue	Users	Revenue	Users	Revenue	Users
	100 0.13% of total	\$0.00 0% of total	8,763 11.67% of total	\$6,040.76 1.27% of total	7,481 9.96% of total	\$203,018.78 42.8% of total	6,704 8.93% of total	\$14,398.22 3.04% of total	1 +0.01% of total
United States	14	\$0.00	2,002	\$5,700.80	4,789	\$194,592.14	2,226	\$13,978.26	0
India	29	\$0.00	1,249	\$0.00	241	\$0.00			1
United Kingdom	1	\$0.00	288	\$0.00	250	\$664.59	326	\$0.00	0
Canada	0	\$0.00	207	\$199.00	199	\$2,137.59	235	\$338.00	0
Japan	3	\$0.00	188	\$0.00	112	\$238.00	275	\$0.00	0
Germany	0	\$0.00	107	\$0.00	115	\$119.00	307	\$0.00	0
Brazil	7	\$0.00	323	\$55.97	55	\$0.00	101	\$0.00	0
France	1	\$0.00	158	\$0.00	164	\$19.19	221	\$0.00	0
Taiwan	2	\$0.00	133	\$0.00	97	\$0.00	260	\$59.97	0
Mexico	2	\$0.00	199	\$59.99	63	\$765.00	69	\$0.00	0

Right click on visualization to interact with data





www.worldpay-globalpaymentreports.com

<https://www.hostinger.co.uk/>

<https://www.hostinger.co.uk/tutorials/build-website-with-chatgpt/>

<https://www.hostinger.co.uk/tutorials/best-ecommerce-platform>

<https://www.hostinger.co.uk/tutorials/ecommerce>

<https://www.hostinger.co.uk/tutorials/make-money-online/>

<https://www.sendcloud.com/>

<https://frontiermarketingllc.com/>

<https://ecommercefastlane.com/>

<https://marketinginsidergroup.com/>

<https://digitalmarketinginstitute.com>

<https://www.simplilearn.com/master-in-digital-marketing>

<https://www.digitalmarketer.com/digital-marketing>

<https://www.socialmediacollege.com/>

***eMarketing Institute: Social Media Marketing, Copenhagen, 2018

G Heggde, G Shainesh: Social Media Marketing, Palgrave

Macmillan, ISBN 978-981-10-5322-1, 2018

B Antczak: The influence of digital marketing and social media

marketing on consumer buying behavior, WSGE University of Applied Science in Jozefow, DOI: doi.org/10.13166/jms/189429, Poland, 2024

MD Prasetya, P ananda, BK Ananda, Fadli: The evolution of social media marketing: a comprehensive systematic review of current

trends, challenges and future insights, Jurnal Pteknologi Kejuruan, V8 N2, pp103-126, DOI: doi.org/10.13166/jms/189429, 2025

N Rawangngnam, P Pongsakornrungsil a o: Social Media and consumer engagement: A bibliometric anaysis and future research directions, Innovative Marketing Journal, Vol 21, Iss3, 2025

SH Siddiquee, M Ali: Exploring the landscape: The societal impact of social media marketing, Academic journal on business

administration, innovation and sustainability, Vol 4, Iss 3, pp94-103, DOI: doi.org/10.13166/jms/189429, 2024

Cuprins

I. Comerțul electronic	1
Perspectiva sell-side	10
II. Noțiunea de Web 2.0	19
Caracteristici ale Web 2.0	20
III. Economia digitală din perspectivă tehnologică	23
Tehnologia internetului	24
Consortiul W3C	27
Scurt istoric	29
Principiile organizației W3C referitoare la internet	32
IV. Browsere web	36
Mozilla firefox	37
Opera	39
Google chrome	40
V. Plăți online	58
Avantaje și dezavantaje ale plăților online	59
Cardurile de credit	61
Tehnologia NFC	62
Banca online	63
Plăți mobile	64
Carduri preplătite	65
Portofele electronice	65
Cecurile electronice	66
Criptomonedele	67

Realizarea unei plăți electronice	69
Măsuri de securitate	71
Procesatoare de plăți online	72
Vulnerabilități în comerțul electronic	75
Vânzarea online	78
Protecția terminalelor tehnologice	79
Recomandări pentru plata pe internet	80
Open web application security project	85
Dicționar de cuvinte privitoare la amenințările informatice	96
VI. Content management systems (CMS)	98
Securitatea CMS	100
ECM/WCM	109
Beneficiile și importanță ECM	111
Ciclul de viață al unui ECM	115
ECM din punctul de vedere al organizației	117
Funcțiile ECM	121
VII. Social Media și Google Analytics	126
Statistici Facebook	128
Trenduri de e-commerce în 2023	131
Ce înseamnă marketingul digital în 2023?	133
Trenduri social media și influenceri	134
Trenduri de e-commerce în 2024-2025	137
Google Analytics	146