CTI Jelentés

A CMS rendszerek biztonsága

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
1996
Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

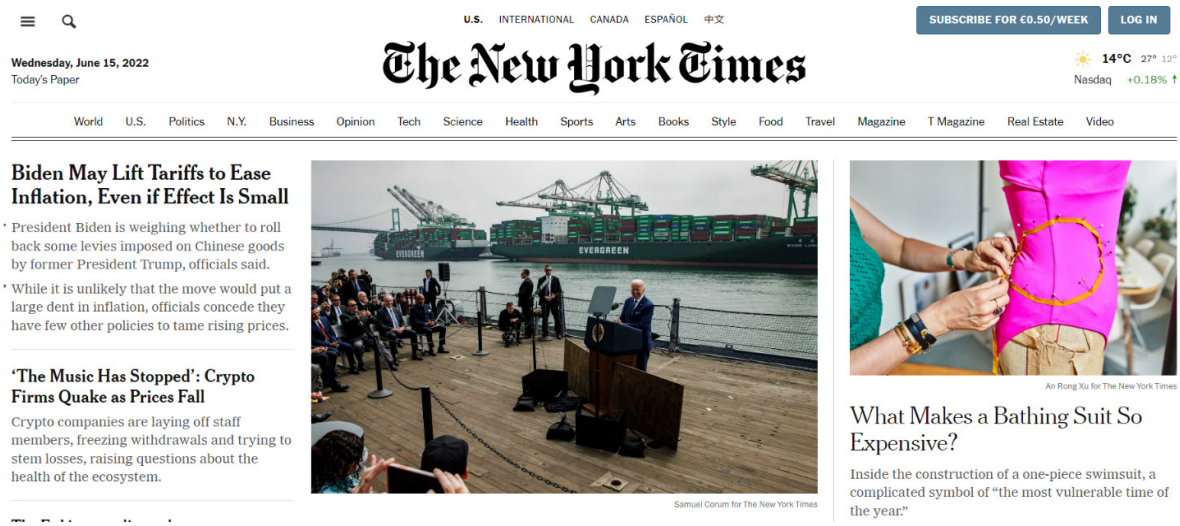
Tartalomjegyzék

Bevezetés

A tartalomkezelő rendszerek (Content Managment System – CMS) olyan szoftverek, amelyek segítségével különösebb webfejlesztői tudás nélkül építhetünk weboldalakat. Számos ilyen platform létezik, és évente hoznak létre újakat. Ezek jellemzően Java, PHP, Microsoft ASP.NET, Perl és Python programozási nyelveken készülnek. Jelenleg a legnépszerűbbek közé tartozik a WordPress, a Shopify, a Wix, a Squarespace, a Joomla és a Drupal.

Jelentőségük évről évre nő, egyre nagyobb arányban találhatók meg azok a weboldalak, amelyek valamilyen CMS platformra épülnek.

A WordPress oldalak a jól tervezettségüknek köszönhetően gyorsan betöltődnek, nem is gondolnánk, hogy hány milliós látogatottságú weboldal épül CMS rendszerre, többek között például a New York Times, a BBC, a CNN, a Sony Music, a Playstation Blog, a Disney Books, vagy a The Rolling Stones oldala is.

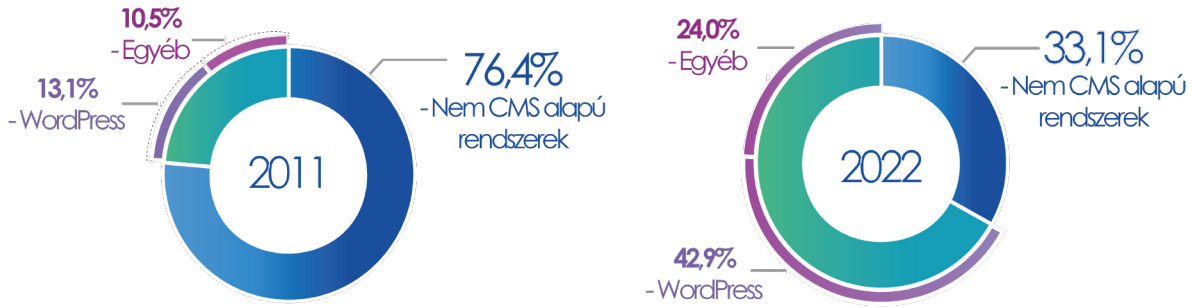


A New York Times nyitóoldala

A W3Techs nyomon követi, hogy az egyes platformok milyen arányban oszlanak meg egymás, illetve más felépítésű weboldalak között.

Míg 2011-ben az összes honlap közül még csak 23,6%-ot tettek ki a tartalomkezelő rendszerek — és ennek több mint a felét a WordPress —, addig 2022 elején már 66,2%-ot — ebből pedig 65% WordPress.

Gyakorlatilag manapság a teljes weboldalpiac 43%-a WordPress tartalomkezelő rendszeren érhető el, minden más, nem CMS alapú rendszer a piac 33%-át teszi ki. A maradék 24%-on osztozik az összes többi, több száz tartalomkezelő rendszer. Ezekből az adatokból jól látszódik, hogy növekvő tendenciát mutat ezen platformok (különösképp a WordPress) népszerűsége, és egyelőre nincs jele annak, hogy ez a tendencia a jövőben változna.



Weboldalak megoszlása 2011-ben és 2022-ben

Mindezek fényében különösen fontossá vált, hogy megfelelő védelemmel lássuk el a CMS alapokon nyugvó weboldalakat is. Jelen dokumentum célja, hogy bemutassa az olvasó számára a CMS rendszerek előnyeit és hátrányait, valamint tanácsokat adjon arra, hogy hogyan tehetjük igazán biztonságossá a honlapunkat, legyen az egy egyszerű blog vagy akár egy összetett, nagy forgalmat generáló webshop. A tájékoztató fókuszába a legnépszerűbb platformot, a WordPresst helyeztük, amelynek megvannak a maga sajátosságai, és bizonyos dolgokban eltér a versenytársaitól, azonban a bemutatásra kerülő „praktikák" általánosan is alkalmazhatóak.

A CMS jellemzői

Bármilyen programozási nyelvről is beszélünk, mindegyiknek vannak előnyei és hátrányai. Ugyanez igaz a CMS rendszerekre is, azonban ezt érdemes két részre bontani.

Az egyik fontos szempont, hogy a CMS-ek között is vannak jócskán eltérő rendszerek, és egyáltalán nem biztos, hogy bármilyen tartalomkezelő megfelelő lesz a célunknak. Például, ha csak blogolni szeretnénk, akkor a reszponzív és letisztult megjelenésű Ghost remek választás lehet, azonban, ha például minket bíznak meg egy iskola honlapjának elkészítésével, akkor a következő szempontok miatt érdemes lehet a Drupallal dolgozni:

- több száz aloldal és nagy mennyiségű adat kezelésére alkalmas,
- biztosítja a többnyelvűséget,
- hatékony tartalom- és felhasználómenedzsmenttel rendelkezik
- és megfizethető funkciók tömbkellegét biztosítja.

Az intézmény jellegéből adódóan a felhasználók rengeteg féle eszközzel rendelkezhetnek, amivel elkívánják érni az oldalt, ezért a Drupal 9-es verziójával épített weboldalak a különböző képernyőfelbontásokra való optimalizáltsága miatt kiváló választás lehet. A Google Analytics modulja pedig lehetővé teszi, hogy összegyűjtsük a felhasználók adatait a tartalomoptimalizálás javítása érdekében.

Rengeteg lehetőség érhető el a piacon, ezért elsősorban érdemes alaposan átgondolni, hogy pontosan mire is van szükségünk, majd csak ezután célszerű kiválasztani a megfelelő platformot. Ezen felül javasolt felmérni az igényeket a dizájnolási, az adathordozhatósági, a bővítmények és a support lehetőségek tekintetében is. Hogy egy örökbecsű közmondást idézzünk: ne a gombhoz varjuk hozzá a kabátot!

A másik lényeges tényező, amely többnyire hátrányként jelenik meg az ilyen oldalaknál, az a megfelelő védelem hiánya. Le kell szögezni, hogy a CMS gyártók és kezelők között is léteznek professzionális megoldások, és az is igaz, hogy attól még, hogy egy oldal PHP-ban készült, egyáltalán nem biztos, hogy jobb, biztonságosabb és felhasználóbarátabb egy WordPress oldalnál. A mai webfejlesztők és alkalmazásfejlesztők is ritkán dolgoznak natív nyelvekkel, előszeretettel használnak jól megírt keretrendszereket, amelyek megkönnyítik a munkájukat, azonban ezeket is jól kell tudni használni. Ebben a tekintetben a webfejlesztők a tartalomkezelő szoftvereket használókkal szemben előnyt élveznek, ugyanis mélyebb technikai tudással rendelkez(het)nek, amely segítségével lépésről lépésre biztonságossá tudják tenni az adott oldalt. A megfelelő időráfordítással egy átlagos felhasználó is képes lehet biztonságossá tenni a CMS oldalakat.

A CMS weboldlak előnyei

- A tartalomkezelők első, és talán a legfontosabb tulajdonsága a felhasználóbarát kezelés. Az ún. „fogd és vidd" (drag and drop) módszer az informatika számos területén egy olyan lehetőséget kínál a felhasználóknak és fejlesztőknek, amivel kódolás nélkül, egy grafikus felületen hajthatóak végre különböző szerkesztési műveletek. A WordPressnek is rendelkezik beépített szerkesztővel, de léteznek hozzá olyan bővítmények, amelyek még ennél is kényelmesebbé teszik a használatukat (például Elementor).

A bővítmények olyan szoftverek, amelyek kibővített funkcionalitást biztosítanak az adott program számára. A fejlesztők az évek alatt rengeteg plugint valósítottak meg, amelyek eredetileg nem képezték részét az adott CMS-nek. Ezeket csak be kell integrálni a weboldalba és használatra készen is állnak anélkül, hogy kódolni kellene hozzá.

- A nyílt forráskódú CMS-ek ingyenesen használhatók.
- A nyílt forráskódú CMS-ek fejlesztésében sok ezer felhasználó vesz részt, a legelterjedtebbekében pedig világszerte akár több százezren is. Ennek számtalan előnye van, például időnként könnyedén megújíthatjuk az oldalunkat az aktuális trendeknek megfelelően.
- A honlap tulajdonosa gyorsan, akár support nélkül képes különféle változtatásokat végrehajtani. Ahogy a CMS neve is sugallja, a legfőbb célja ezeknek az oldalaknak a tartalmak kezelése, így elengedhetetlen, hogy könnyedén tudjunk az igényeink szerint módosítani a szükséges elemeken, tartalmakon.

- Bármilyen funkciót is töltsön be a létrehozott oldal, valószínűleg érdekünk fog fűződni ahhoz, hogy minél többen és minél könnyebben rátaláljanak egy keresés során. Ebben segít az úgynevezett keresőoptimalizálás, vagyis a SEO (Search Engine Optimization).

- A rendelkezésre álló bővítményekkel könnyedén optimalizálhatjuk ezeket az oldalakat, amivel növelhetjük weboldalunk „láthatóságát" a keresési találatok között.

- A felhasználói élmény maximalizálása rendkívül fontos a weboldalak esetén, hiszen ha a felhasználónak tetszik az oldal, és azon kényelmesen eligazodik, az lényegesen növeli annak esélyét, hogy „vevővé konvertálódjon", mintha például mobilfelületen szétcsúszna az oldal. Ez tökéletesen megoldható CMS-ekkel.

Mi az a konverziós ráta?

Az a százalékos arány, amikor a felhasználók egy adott része végrehajtja a kívánt műveletet, például vásárol az oldalon vagy feliratkozik a hírlevelekre.

A CMS weboldlak hátrányai

- A felhasználóknak a legtöbb funkcionalitás tekintetében a bővítményekre kell támaszkodniuk, azaz a CMS-ek ezen előnye egyben hátrányukat is jelenti. Bár rengeteg ingyenes bővítmény érhető el, ám ezek sok esetben csak fizetős szolgáltatásként vehetők igénybe.

- A tartalomkezelők egy másik előnye is könnyen a hátrányukká válhat: mivel a weboldalak kétharmada valamilyen CMS-re épül, amelyek széleskörben ismertek, így tömeges célpontjai lehetnek a kiberbűnözőknek. Azok a támadók, akik ilyen rendszereket céloznak, nagy valószínűséggel ismerik a sebezhető pontokat, és akár tömegesen is kihasználhatják azokat.

- Egy CMS-sel tervezett weboldal betöltési sebessége jelentősen elmaradhat más fejlesztési módokhoz képest.

- A legtöbb rendszer korlátozott számú felhasználót képes fenntartani. Amikor az oldal látogatottsága nagy mértékben megnő, előfordul, hogy nehézkessé válik a skálázás, vagyis problémát okozhat a megnövekedett terhelés kiszolgálása. Ilyenkor elképzelhető, hogy egy másik rendszerre kell váltani, hogy ne romoljon a felhasználói élmény.

- Sok időbe telhet az oldal tervezőjének, hogy megtaláljon egy esetleges hibaforrást. Elképzelhető, hogy olyan hibába ütközik amire az egyetlen megoldás a teljes oldal újratervezése.

- A CMS oldalak elsősorban sablonokra épülnek, ezért bizonyos értelembe véve nem is túl rugalmasak a tervezést tekintve.

- Mivel egy CMS webhely adatbázis alapú, meg kell várni, amíg a szerver feldolgozza az oldalakat. Több száz oldal esetén lassú lehet a betöltésük, ami a látogatók elvesztéséhez vezethet. A Hobo Seo Consultancy tanulmányából kiderül , hogy 2 másodperc alatti betöltési idő az ideális egy honlap esetén. Ha ez 3 másodpercnél tovább tart, akkor a látogatók több mint fele elhagyja az oldalt és minden tized másodperccel ez a szám drasztikusan nő.

WordPress

Fontos megjegyezni, hogy a WordPress alatt a WordPress.org-ot értjük, és nem a WordPress.com-ot, a kettő nem ugyanaz. Eredetileg a WordPress.org-ot blogolásra tervezték, azonban az évek alatt olyannyira átalakult, hogy mára már bármilyen oldal létrehozására alkalmassá vált. Ezt használják a legtöbben és ehhez érhető el a legtöbb bővítmény is. A WordPress.com egy blog hosting szolgáltató, és nem áll közvetlen kapcsolatban a WordPress.org-gal.

A WordPress hatalmas pozitívuma egyrészt a könnyű kezelhetősége, másrészt a gyors változtatásra való képessége. A WordPresst, mint keretrendszert saját vagy bérelt webtárhelyre tudjuk feltelepíteni. A tárhelyszolgáltatók szinte kivétel nélkül biztosítják, hogy percek alatt installálható legyen a WordPress. Érdemes azonban megjegyezni, hogy nem ajánlott ingyenes tárhelyszolgáltatót használni! E célból válasszunk inkább egy megbízható hosting szolgáltatást! Éves szinten ennek költsége nagyjából egy prémium WordPress téma (theme) költségének felel meg (100 dollár alatt) az adott csomagtól és szolgáltatótól függően. Ezzel a témával egy külön fejezetben (Webtárhelyek) részletesebben is foglalkozunk.

A legtöbb WordPress bővítményt a SEO céljaira tervezték, könnyedén megérthetők a Meta tagek használata, amelynek célja, hogy egy releváns kereséssel minél többet rátaláljanak az oldalara. Rengeteg ingyenes és prémium téma, valamint bővítmény érhető el, ezért kiváló választás lehet az éppen induló vállalkozások számára. Továbbá a WordPresshez rendszeresen érkezik verziófrissítés, viszont előfordulhat, hogy a gyakori frissítések problémákat okoznak a szolgáltatásokban.

WordPress hardening

– avagy hogyan fokozzuk a weboldalunk biztonságát?

Mint minden weboldalnál, így a WordPress-alapú rendszereknél is nagyon sarkalatos pont a megfelelő biztonság kialakítása. Alaposan járjuk körbe ezt a témát, mielőtt weboldal építésbe fogunk, ugyanis vállalkozásunk jóhíre és hitelessége múlhat a felkészültségünkön. Jobb elkerülni, hogy anyagi és reputációs kár érjen bennünket, ezért érdemes odafigyelni néhány dologra. A WP oldalak ellen a leggyakoribb támadások:

- DDoS, azaz túlterheléses támadások,
- sebezhető bővítmények és témák elleni támadások,
- cookie fájlokat érintő támadások,
- befecskendezéses támadások és
- adathalászat.

Ebben a fejezetben olyan praktikákat és módszereket mutatunk be, amelyek betartásával jelentősen csökkenthetők a fent felsorolt támadások sikeres bekövetkezésének valószerűsége.Az NBSZ NKI által felsorolt tanácsok mellett az egyik legfontosabb, hogy maradjunk naprakészek, és kövessük figyelemmel a választott CMS rendszert érintő aktuális sebezhetőségről és biztonsági frissítésekről szóló információkat.

Ha például értékesíteni szeretnénk a honlapunkon, gondoljunk arra úgy, mint egy fizikai üzletre: nem elég felszerelni a kamerákat és a riasztókat, folyamatosan karban kell tartani és felügyelni kell azokat, hogy megóvjuk magunkat a rosszindulatú szereplőktől. A kiberbűnözők nagy erőfeszítéseket tesznek azért, hogy megtalálják a sebezhető rendszereket, éppen ezért elengedhetetlen, hogy ellássuk az oldalunkat a megfelelő védelemmel.

Amikor egy weboldal biztonságának kialakításához jutunk, érdemes néhány alapvető szabályt betartani:

- Készítsünk rendszeresen biztonsági mentéseket az oldalról, hogy az egy esetleges hackelés után a lehető leghamarabb újra elérhető lehessen!
- Lehetőleg a bővítményeket és a témákat csak a WordPress.org-ról szerezzük be, ne telepítsünk más forrásból származó modulokat! Törekedjünk minél kevesebb, csak a legszükségesebb bővítmények alkalmazására!
- Az általunk használt számítógépeket is fontos karban tartani és jogtiszta, megbízható vírusírtóval ellátni. Hiába a sok erőfeszítés, ha a számítógépünket megfertőzi egy kártevő, és azon keresztül érik el a honlapunkat.
- Mindig tartsuk naprakészen az operációs rendszerünket, a használt szoftvereket és webböngészőnket!

- Ha érkezik egy frissítés a WordPresshez, a lehető leghamarabb telepítsük és ügyeljünk arra, hogy ezt mindig a https://wordpress.org/ oldalról szerezzük be! Ha egy új sebezhetőséget fedeznek fel a WordPressben, és ezt egy új verzió kiadásával orvosolják, a sebezhetőség kihasználásához szükséges információk szinte mindig nyilvánosságra kerülnek, ezáltal a régi verziók nyitottabbá válnak a támadásokkal szemben.

- Tájékozódjunk a különféle kiberbiztonsággal foglalkozó honlapokon az aktuális sérülékenységekről!

- Az admin fiókhoz válasszunk erős, egyedi jelszót! Figyeljünk arra, hogy ez soha ne értelmes szó legyen, mert ezeket a nyers erővel való támadások során jóval könnyebben törik fel.

- Soha ne lépjünk be az adminisztrációs felületre nyílt hálózaton keresztül, mert egy titkosítatlan kapcsolaton keresztül lehallgathatják a hálózati forgalmat, és megszerezhetik a jelszavunkat!

- Ha a webtárhelye biztosítja, érdemes FTP helyett SFTP-t (Secure File Transfer Protocol) használni, hogy az adatátvitel titkosítva történjen.

- Az adatbázis kezelőknek a normál WordPress műveletek végrehajtásához (tartalomlétrehozás, fájlok feltöltése, hozzászólások és felhasználók kezelése, bővítmények telepítése stb.) elegendő csak CRUD (CREATE, READ, UPDATE, DELETE) jogosultságokat adnunk, adminisztrációs jogköröket ne adjunk nekik (DROP, GRANT, ALTER)!

- A WordPress Dashboardon lehetséges a PHP fájlok (bővítmények, témák) szerkesztése. Ezt kétféleképpen tilthatjuk le: vagy beírjuk ezt a sort a wp-config.php-ba: "define('DISALLOW_FILE_EDIT', true);", vagy eltávolítjuk az 'edit_themes', 'edit_plugins' és 'edit_files' tulajdonságokat, így senki nem fog tudni bővítményeket, témákat és fájlokat szerkeszteni.

- Mindig legyenek frissítve a bővítmények!

- Telepítsünk tűzfalat! A webalkalmazás tűzfalak (WAF) alapvető biztonságot nyújtanak az oldalunknak. Léteznek DNS és alkalmazás-szintű tűzfalak. Míg előbbinél a forgalom keresztül van irányítva annak felhő proxy szerverein, és ott kerülnek szűrésre a káros tartalmak, addig az utóbbinál a WP szkriptek lefutása előtt kerül ellenőrzésre a forgalom. A legnépszerűbb tűzfal pluginok közé tartozik a Cloudflare, a MalCare, a Wordfence, a Sucuri és a SiteLock.

- Limitáljuk a bejelentkezési próbálkozásokat! Alapértelmezetten a WordPressnél korlátlanul lehet próbálkozni a bejelentkezés során, ami a brute force támadások melegágya. Például a Login LockDown nevű plugint telepítve könnyedén beállíthatjuk, hogy adott számú sikertelen próbálkozás után csak egy bizonyos idő elteltével tudjon ismét próbálkozni a felhasználó, aki rossz jelszóval próbálkozott. Amennyiben nem adunk meg ilyen megkötést, a támadók másodpercenként több ezerszer, - komolyabb hardverekkel vagy botnetekkel - akár több milliószor is próbálkozhatnak. Ezenfelül érdemes az XML-RPC-t kikapcsolni, mert a system.multicall funkcióval néhány kéréssel több százszor próbálkozhat a támadó.

- Használjunk kétfaktoros hitelesítést (2 Factor Authentication – 2FA)! Ilyenkor a szokásos felhasználónév-jelszó pároson kívül, egy második faktor is szükséges a hietlesítéshez. Ez általában egy külön alkalmazásban vagy eszközön történő további hitelesítési forma. Elterjedt megoldás, amikor SMS-ben vagy e-mailben kerül kiküldésre egy karaktersorozat, amit a felhasználónak meg kell adnia a sikeres bejelentkezés érdekében. Plusz védelmet biztosít, ha arra is időlimitet állítunk be, hogy mennyi ideje lehet a felhasználónak megadnia ezt a kiküldött kódot. A legelterjedtebb 2FA pluginok a Shield WordPress Security, Google Authenticator, Two-Factor Authentication, Wordfence Security és az iThemes Security Pro, amelyek között például a Wordfence – csökkentett funkciókkal bár, de ingyenesen is elérhető, és az admin oldalunk kétfaktoros védelmét is képes ellátni.

- Ha valamilyen rendellenességet fedeztünk fel, fontos manuális scannelést végrehajtani az oldalunkon, de ezt javasolt időközönként akkor is elvégezni, ha egyébként nem tapasztalunk problémát. Erre alkalmas toolok például a WPSec, ScanWP, Sucuri SiteCheck vagy a WordPress Security Scan.

- Abban az esetben, ha támadás áldozata lett az oldalunk, mindenképpen keressünk fel egy szakembert, mert elképzelhető, hogy olyan hátsó ajtókat (backdoor) helyezett el a támadó, hogy egy esetleges sikeres helyreállítás után is hozzáférést biztosít önmagának az admin felülethez!

Webtárhelyek

Amikor weboldal építésbe kezdünk, sarkalatos pont, hogy milyen tárhelyszolgáltatót választunk. Az első és legfontosabb, hogy soha ne válasszunk ingyenes szolgáltatókat, mert bár vonzó lehet egy induló kisvállalkozás számára olyan szempontból, hogy ingyen hozzájuthat, a későbbiekben szinte biztosan csak a gond lesz vele. Ilyen probléma lehet például, hogy a felhasználó nem rendelkezik root vagy rendszergazdai jogosultságokkal, nehézkes vagy lehetetlen SEO optimalizálás, az oldalt adott esetekben nem lehet átköltöztetni, ha arra lenne szükségünk és teljes mértékben megbízhatatlan a jövőt illetően. Mivel nem fizettünk semmiért, reklamálni sem tudunk, ha például egyik napról a másikra teljesen eltűnnek a tárolt adataink.

A legnépszerűbb webtárhelyszolgáltatások típusukat tekintve a következők lehetnek:

- Megosztott: több webhely is helyet kap egy szerveren, és az összes domain a közös erőforrásokon osztozik.
- VPS (virtuális privát szerver): a nagy teljesítményű szerver kisebb virtuális szerverekre van felosztva, hogy optimalizáltan legyenek az erőforrások felhasználva.
- Dedikált: a felhasználónak root/rendszergazdai jogosultsága és teljes irányítása van felette. Ez az egyik legolcsóbb, azonban a bérlője felel a biztonságáért.

- Menedzselt: a dedikált ellentétje, vagyis a felhasználónak nincs teljes hozzáférése, azonban cserébe a szolgáltató biztosítja a karbantartást, a biztonságot és a szolgáltatás minőségét.
- Cloud (felhőalapú): manapság az egyik legnépszerűbb fajtája a tárhelyszolgáltatásoknak. Megbízható, és könnyen skálázható, a ténylegesen felhasznált erőforrásmennyiség utáni fizetés jellemzi.

Mindenképpen érdemes alaposan utánajárni vásárlás előtt, hogy számunkra ki lehet a legmegfelelőbb szolgáltató. Ilyen tényező lehet az SSL megléte, a szolgáltatás által nyújtott támogatás (support), biztosított domainek száma, a tárhely mérete, maximális sávszélesség, szolgáltatott IP címek száma, elérhető csomagok, az ezek közti esetleges váltásnak a lehetősége és természetesen az ár. Rendelkezésre állási időt tekintve nagyjából az összes szolgáltató 99,9%-ot ígér, amellyel éves szinten 9 óra leállást engednek meg maguknak. A teljesség igénye nélkül a legnépszerűbb WordPressre specializált tárhelyszolgáltatók közé tartozik a BlueHost, Hostinger, DreamHost, SiteGround és a CloudWays.

A tárhelyszolgáltatók általában több olyan népszerű, széleskörben használt modult is biztosítanak, amivel kényelmessé és egyszerűvé teszik a telepítést, konfigurációt és a mindennapos feladatainkat:

- cPanel: Egyszerű webes felületet biztosít a tárhely fiókok kezeléséhez.
- Softaculous: A Softaculous egy népszerű automatikus telepítő szkript, segítségével könnyedén telepíthető a WordPress és más webes alkalmazások.
- QuickInstall: Ez egy másik népszerű automatikus telepítő, a Softaculous alternatívája.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022