Kérdések

Általános kérdések

1.) Lehet aláhúzás domain névben?

2.) Ki jogosult a '.' (root) zónát szerkeszteni, ki férhet hozzá?

3.) Lehetséges, hogy az összes - 13 db - internet root névszerver egyszerre elérhetetlen legyen? Mondjuk egy jól összehangolt támadás következtében?

4.) Milyen szempont alapján válasszak névszerver szolgáltatót, amennyiben fontos, értékkel bíró domain névvel rendelkezem?

5.) Van e tekintetben különbség egyáltalán a névszerver szolgáltatók között?

6.) Nem szeretném, hogy a védjegyemmel megegyező domainnevet Európa országainak TLD-je alá regisztrálják; érdemes minden európai országban bejegyezni saját részre? Milyen lehetőségeim vannak a védelemre?

7.) Nem került hosszabbításra a domainnevem fenntartása, a Regisztrátortól nem kaptam értesítést a fenntartás hosszabbítás aktualitásáról. Köteles a Regisztrátor értesíteni? Felelősségre vonható az ebből eredő kárért?

8.) Mit tud tenni a .hu Nyilvántartó a csalárd domain megszerzés ellen?

9.) Laikusként hogyan ellenőrizhetem legegyszerűbben, hogy a kapott e-mail feladója valóban az, aki küldte. Érvényes DKIM aláírás elegendő ehhez?

10.) A DNSSEC mivel nyújt nagyobb védelmet a számomra?

11.) Szolgáltatóm DNS szerverei egyben webszerverek is. Helyes-e ez?

12.) Szolgáltatóm csak két névszervert alkalmaz. Elégséges-e ez?

INTEGRITY Kft. szolgáltatásaival kapcsolatos kérdések

1.) Mit biztosít az INTEGRITY Kft. névszerver szolgáltatás alatt?

2.) Hogyan biztosítja az az INTEGRITY Kft., hogy illetéktelen ne kérhessen jogosulatlan DNS szintű módosítást a domainnevem esetén?

Kérdések és válaszok

1.) Lehet aláhúzás domain névben?

A **helyes válasz igen**, de ez nem jelenti azt, hogy .eu alá most már regisztrálhatjuk is az alábbi domainnevet:
ez_a_kedvencem.eu, mert nem. Lásd alább az indoklást.

Az RFC 2181, section 11, "Name syntax" szerint:
"The DNS itself places only one restriction on the particular labels that can be used to identify resource records. That one restriction relates to the length of the label and the full name. [...] Implementations of the DNS protocols must not place any restrictions on the labels that can be used. In particular, DNS servers must not refuse to serve a zone because it contains labels that might not be acceptable to some DNS client programs."

Azaz **doménnév címkéjében megengedett az aláhúzásjel**.

Nem csak megengedett, hanem rendszeresen használatos is, pl.:

mail._domainkey.integrity.hu

És ez rendjén működik is:

PS> resolve-dnsname -server dns1.hu -name mail._domainkey.integrity.hu -type txt

```
Name                           Type   TTL   Section    Strings
----                           ----   ---   -------    -------
mail._domainkey.integrity.hu   TXT    3600  Answer     {v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQ
                                      EFAAOCAQ8AMIIBCgKCAQEA2EYk7AfNqbp+6YCrnRy
                                      sU15sEimURA6isVpi7hoL363hrKzzhxl434nPEbiP
                                      epbwqUDK/k7h6WBOhLniywulap+4+4Sxf2XwJB0Yw
                                      vmxn0shnWGNK1qQfWlQrhb8OMrF8wsiOocTDuYq8n
                                      uiHoJcuO3zXie9yBcCGh4C/JrZATAnwVhp/lxXiqA
                                      AcBoE3HLrZ, cIVy8yA5HV4PAcNlkIHkJY2Y/WHNh
                                      BKaQql6fNJ/M8x5BbLIp0MGOzCAyfMF76wFAmWr0M
                                      WCeShkgF2zFJqGgJP2BYkppIJSsUVgVyvHEIMnWQb
                                      jneq5Vp/lLmNEUsgAy7nkGgLOTC/B7ToJzhprQIDA
                                      QAB}
```

Fontos viszont tudni azt, hogy **hosztnévben nem megengedett**, a releváns RFC, az RFC 1123 hosztnévben csak angol betűket, decimális számokat és kötőjeleket enged meg.

TLD-k alá nem megengedett általában olyan címke regisztrációja, mely nem tesz eleget az RFC 1123 hosztnevekre szóló megkötésének. (Sajnos az aláhúzásjelet méltatlanul diszkvalifikálják a TLD-Registry-k :-)

2.) Ki jogosult a '.' (root) zónát szerkeszteni, ki férhet hozzá?

Az **Internet Corporation for Assigned Names and Numbers (ICANN)** szerkeszti és publikálja a hivatalos root zónafile-t, melyet a root névszerverek szinkronizálnak.

Itt elérhető a hivatalos root zónafile:
https://www.internic.net/zones/root.zone

Részletesebb választ ad a Wikipedia:
"Since 2016, the root zone has been overseen by the Internet Corporation for Assigned Names and Numbers (ICANN) which delegates the management to a subsidiary acting as the Internet Assigned Numbers Authority (IANA).[1] Distribution services are provided by Verisign."
https://en.wikipedia.org/wiki/DNS_root_zone

3.) Lehetséges, hogy az összes - 13 db - internet root névszerver egyszerre elérhetetlen legyen? Mondjuk egy jól összehangolt támadás következtében?

Elvben lehetséges, de a root névszerver-kiszolgálás nagyon védett mind véletlen hibák, mind szándékos károkozás ellen. Lássuk, hogyan:

Nem 13, hanem több mint 1000 névszerver szolgálja ki a root zónát. Azonos név és IP cím alatt tehát nagyon sok szerver van valójában, köszönhetően az anycast routingnak.

Földrajzilag az egész világon elosztottan helyezkednek el, és nagyon sok egymástól független hálózatra csatlakoznak.

Ezen névszerverek külön-külön viszonylag nagy sávszélességű hálózati kapcsolatokkal rendelkeznek, és erős szerverek.

A névszervereken bizonyos szoftveres DDoS védelmi megoldások is alkalmazottak (pl. rate limit).

A névszervereket 12 független szervezet üzemelteti.

A névszervereken nem egyetlen névszerver szoftver fut, hanem többségükön BIND, kisebb részükön NDS. Szoftverhiba ellen így védett az egész rendszer, nem valószínű, hogy egyszerre érintsen egy biztonsági hiba teljesen különböző névszerver szoftvereket.

A névszerver szoftverek maguk is nagyon megbízhatók, nagyon ellenőrzöttek.

A védelem kifinomultságát jól mutatja, hogy például a DNSSEC kulcsok cseréjét hogy végzik, lásd: DNSSEC Root Signing Ceremony, illetve egy ilyen konkrét ceremóniáról videó: https://youtu.be/B46cWBUU2l4, illetve lásd mit változtatott ezen a Covid-19: https://youtu.be/_yIfMUjv-UU.

Hatékony támadást root névszerverek ellen senkinek nem sikerült még indítani. Noha nincsenek nyugtalanító incidensek, évről évre csak erősítik a root zóna védelmét, pl. folyamatosan növekszik a root névszerverek száma.

4.) Milyen szempont alapján válasszak névszerver szolgáltatót, amennyiben fontos, értékkel bíró domain névvel rendelkezem?

1. eset: a doménnév fontos, de a DNS szolgáltatás nem fontos hozzá:

Bármennyire is fontos a doménnevünk, a DNS szolgáltatás hozzá csak akkor fontos, ha technikailag is használjuk ezt a doménnevet és ez alatt fontos szolgáltatásukat nyújtunk.

Ha van egy **parkolópályás** nevünk, akkor legjobb, ha ez be sem kerülne a megfelelő TLD zónába, vagy ha bekerül, akkor ez a zóna hamis, nem létező névszerverekre mutat, mely névszervereket nem lehet hamisan üzemeltetni.

Például van egy doménnevünk, a valami.eu,

ha ekkor az eu zónába az alábbi két névszerver lenne megadva
sq86vpv024zcfnz5jv4w.nye1v44hk6a4yq3e5uzp
nye1v44hk6a4yq3e5uzp.sq86vpv024zcfnz5jv4w,

akkor biztosak lehetünk, hogy semmilyen DNS feloldás nem fog történni valami.eu-ra vagy aldoméneire.

(Sajnos a .hu TLD speciális, tiltja és 'bünteti' ezt a megoldást.)

2. eset: a doménnév fontos, és a DNS szolgáltatás is fontos hozzá:

Ha viszont fontos a névszerver-szolgáltatás, akkor olyan névszerver-szolgáltatót érdemes választani, aki várhatóan

- **biztonságos**
- **és megbízható**

szolgáltatást fog nyújtani számunkra.

Lehetnek speciális szempontok, pl.

- az egész Földön jól elérhető, kis válaszidejű névszerver-szolgáltatást akarunk,
- még a Kínai Népköztársaságban is jó elérést akarunk,
- még Iránban is jó elérést akarunk …

Ezen esetekben biztos, hogy worldwide anycast DNS szolgáltatásra is igényünk van.

A névszerver-szolgáltatás lehet ingyenes és fizetős, fizetős szolgáltatás lehet flat díjazású, de lehet lekérdezések száma szerint fizetett is (ilyen pl. az Amazon Route 53, a Google DNS, a Microsoft Azure stb.). Az INTEGRITY Kft. nyújt ingyenes és fizetős, ezen belül flat díjazású és opcionálisan flat + lekérdezésszám alapú díjazású szolgáltatást.

Az biztos, hogy nem könnyű általában megítélni mely szolgáltató nem kellően biztonságos, a megbízhatóságnak még csak-csak könnyű utánanézni. De persze nem könnyű azt sem megítélni, hogy mennyire jó egy webhoszting szolgáltatás, de annyi biztos, ha problémákat látunk körülötte, vagy rossz tapasztalatunk vele, akkor kerüljük el. (Pl. az INTEGRITY Kft. ingyenes DNS szolgáltatásában 2014. óta nem fordult elő olyan másodperc, amikor is legalább egyik névszerver ne lett volna elérhető, 2014-ben volt egy upgrade, mely rövid üzemszünettel járt. Mindazonáltal az INTEGRITY Kft. ingyenes szolgáltatása nincs felkészítve úgy DDoS támadásokra és számos más problémára, mint fizetős ún. Prémium DNS szolgáltatásai.)

5.) Van e tekintetben különbség egyáltalán a névszerver szolgáltatók között?

Hogyne, nagyon is van!

Egy Trabant és egy Rollce-Royce között könnyen különbséget tesz bárki. Noha névszerver szolgáltatások között nem ilyen szembeötlő a különbség, gyakran nagyon is jól látható, megállapítható.

Elsőként kézenfekvő azt nézni, hogy pl. DNSSEC támogatott-e (DNSSEC-et nyújtó DNS szolgáltató ettől még lehet rosszabb, egy azt nem nyújtónál, de rossz jel, ha egy DNS szolgáltató ilyet nem nyújt, másrészt fontos doménnevünkhöz nyilván nem választunk olyan névszerver-szolgáltatót aki nem nyújt DNSSEC-et).

Csinálhatunk pár ellenőrzést, és ha hibákat, kétes dolgokat tár fel, akkor megfontolandó adott névszerver-szolgáltató elkerülése.

Nézzük meg, hogy hány névszerver szolgál ki. Ez nem triviális, hiszen anycast DNS szerverek azonos hosztnéven és azonos IP címeken érhetők el. Ökölszabály, csak kettő névszerver van, és ezek nem anycast névszerverek, akkor még lehet elég jó számunkra a névszerver szolgáltaáts, de óvatosságra intő a csak két névszerver ténye.

A biztonság terén is sok árulkodó jel lehet, sajnos általában nehéz mit mondani, konkrét szolgáltatások már viszont összehasonlíthatók.

Másrészt az igények is mások, egy extrém forgalmú webáruház vagy egy online banki fizetés site-ja másabb névszerviz-szolgáltatást érdemel, mint egy fontos, de nem ennyire kritikus.

Egy nagyvállalat igényei is mások lehetnek, mint egy tipikus kisvállalaté, pl. eg nagyvállalalat saját hidden kliens névszerverről szeretne szolgáltatón keresztül publikus DNS szolgáltatást kívánhat nyújtani, vagy kis vállalat lévén, ez túlzás lenne számára, költség vagy menedzsment okokból ez nem lenne praktikus. Azonban azt sem mondtuk, hogy nagyvállalatoknak általában saját hidden DNS szervert kell, hogy üzemeltessenek, ez egy lehetőség a sok közül, adott esetben lehet éppen egy nagyon jó lehetőség is.

6.) Nem szeretném, hogy a védjegyemmel megegyező domainnevet Európa országainak TLD-je alá regisztrálják; érdemes minden európai országban bejegyezni saját részre? Milyen lehetőségeim vannak a védelemre?

Érdemes-e vagy megéri-e kérdésre a konkrét szereplő és körülmények ismerete hiányában nehéz válaszolni.

Fontos kérdés, hogy az adott országban helyi piacon, helyi nyelven, esetleg helyi képviselettel szeretnénk-e megjelenni.

Lehetőség van arra is, hogy valamily TLD alatt bár nem regisztráljuk a nevet, de ha más regisztrálja, és jogos érdekeinket sértve használja, akkor felléphetünk ellene, felszólíthatjuk (ha ismerjük kilétét), hogy álljon el a jogsértő használattól vagy jogi úton léphetünk fel ellene.

Képzeljük csak el, hogy ez mennyire egyszerű lehet például Albániában vagy Törökországban! - És milyen költséggel járhat?

Adott európai országokban csak nemzeti regisztrátorokon keresztül regisztrálhatunk nevet, így bizonyára az egyetlen járható út, keresni egy közvetítőt aki képes minden vagy legalábbis legtöbb európai országban részünkre nevet regisztrálni.

A nemzeti regisztrátorok mindig jelentenek kockázatot, lehetnek köztük olyanok akiknél a biztonság gyenge lábon áll. Legjobb inkább csak regisztrációval lefoglalni legtöbb országban a doménnevet, de ténylegesen nem használni minden TLD alatt.

Érdekességként megemlítjük, hogy van olyan európai (bár legtöbb állam által nem elismert) ország, a Dnyeszter Menti Moldáv Köztársaság (Transznisztria), mely nem is rendelkezik se kétbetűs ISO országkóddal, se saját TLD-vel. Van olyan 'TLD', az su - Szovjetunió, mely már 'nem létező állam országkódja'. Egyes országoknak, mint pl. Bulgária, Görögország, Szerbia stb. több saját ccTLD-je is van, és magának az Európai Uniónak is három országkódja van, az eu, az .ею és az .ευ. Másrészt lehetnek fontos másodszintű közdomének is, mint pl. a co.uk vagy akár a co.hu, mely alá igényünk lehet regisztrálnunk.

7.) Nem került hosszabbításra a domainnevem fenntartása, a Regisztrátortól nem kaptam értesítést a fenntartás hosszabbítás aktualitásáról. Köteles a Regisztrátor értesíteni? Felelősségre vonható az ebből eredő kárért?

A hosszabbításról az előfizető dönt, ha abban állapodik meg regisztrátorával, hogy lejárat esetén regisztrátora értesítést küldjön, akkor regisztrátora köteles értesítést küldeni.

Regisztrátorok akkor is szoktak e-mailen értesítést küldeni lejáratról, ha nem is vállalnak kötelezettséget értesítés küldésére.

Ha e-mailen küld regisztrátor értesítést, akkor gyakran előfordul, hogy bár a regisztrátor küld értesítést, a címzett vagy az őt kiszolgáló szerver nem fogadta a levelet, vagy bár a levél akár kézbesítésre is került, de a címzett azt nem olvasta (például amiatt, mert spamfolderbe került a levél).

E-mail értesítések kényelmi jelentőségűek, domén fenntartás hosszabbítását nem erre kellene alapozni.

Másrészt doménfenntartás nem feltétlenül jár le, sok regisztrátor vállal határozatlan időre fenntartást. Határozatlan időre szóló fenntartás esetén nem jár le a domén, azonban az előfordulhat, hogy a díjat az előfizető nem fizeti be, és ekkor a regisztrátor felmondja a fenntartást.

Fontos doménekről gondos doménhasználó nyilván gondos nyilvántartást vezet, ha ezt nem tenné, akkor bizony elvesztheti doménneveit. Sajnos meglepően sokan nem vezetnek nyilvántartást, sőt még viszonylag fontos doménneveikről azt sem tudják, hogy mely regisztrátor tartja fenn részükre.

Sokan a problémákat úgy kívánják elkerülni, hogy hosszú időre előre kifizetik regisztrátoruknak a domainfenntartás díját, de arra ekkor is figyelni kell, hogy a hosszú idő is majd letelik, és akkor hosszabbítani kell a fenntartást vagy határozatlan időre szóló fenntartás esetén a további fenntartás díját meg kell fizetni.

Természetesen regisztrátor felel azért a kárért, ha valamit vállalt, és azt nem megfelelően nyújtotta. Ugyanakkor egy határozatlan időre szóló szolgáltatás szerződés lejárta, ha nem kerül hosszabbításra, azért nyilván az előfizető/doménhasználó az aki elsősorban felelős.

A regisztrátorok ettől függetlenül jellemzően küldenek e-mail értesítést, rendszerint többet is.

Működő doménnevet persze elveszteni nagyon nehéz, például .hu domén esetén a lejárat után még van egy 45 napos grace periódus, amíg a domén a doménhasználó kezelésében marad, majd ezután még jön egy 60 napos periódus, amikor is a korábbi doménhasználó újraregisztrálhatja doménét. A domén DNS-e már erre a periódusra kikerül a .hu zónából, így az nem működik, fontos doménnél nyilván feltűnik, hogy a domén nem működik.

Persze ha a domént valaki nem is veszti el, de átmenetileg a doménhez a DNS szolgáltatás nem működik, abból komoly kár keletkezik. Mint mondtuk elveszteni fontos és működő domaint nem könnyű, komoly szintű gondatlanságot igényel ez a doménhasználó részéről :-(

És igen, előfordult, hogy regisztrátor hibázott, az INTEGRITY Kft-nél is előfordult egy ilyen eset vagy két évtizeddel ezelőtt, de végül is ügyfelünk megelégedésére sikerült rendezni az ügyet, és természetesen tanultunk belőle, hogy ilyen hibát a jövőben elkerüljünk. Az INTEGRITY Kft. lejárat előtt több értesítést is küld, lehet több évre előfizetni nála, lehet határozatlan időre is szerződni, és lehet lejárat elleni speciális védelmi szolgáltatásokra előfizetni, pl. plusz értesítésekre (pl. postai), vagy akár arra, hogy lejáratkor kutasson a doménhasználó után a regisztrátor, ha az nem jelentkezik.

8.) Mit tud tenni a .hu Nyilvántartó a csalárd domain megszerzés ellen?

A .hu Nyilvántartó **többféle registry lock** szolgáltatást is nyújt, melyet regisztrátorok értékesíthetnek ügyfeleik számára.

A **teljeskörű registry lock**, a .hu Nyilvántartó terminológiájában az ún. **doménzár** talán a legerősebb védelmi eszköz amit kínál, sajnálatosan nem népszerű, alig pár regisztrátor szerződött a .hu Nyilvántartóval ennek kínálatára, és nagyon kevés ügyfél veszi ezt igénybe.

A megelőzésen túl, ha már valakinek lenyúlták a doménnevét, akkor a .hu rendszer és a Nyilvántartó más TLD-knél bizonyos tekintetben jobb védelmet nyújt, ugyanis a doménhasználókról egyedi hivatalos azonosítót (tipikusan ez adószám vagy természetes személyek esetén tipikusan személyazonosító okmány azonosító) rögzít a nyilvántartásban, így vita esetén eldönthető pl. hogy két Nagy István közül, aki vitatkozik, hogy kié a doménnév, melyiké is az a nyilvántartás szerint.

A teljeskörű doménzárral kapcsolatban arra szeretnénk felhívni a figyelmet, hogy ennek biztonságos igénybe vétele kellő szervezeti hátteret igényel a doménhasználó részéről. Az INTEGRITY Kft. gyakran azért nem ajánlja a teljeskörű doménzárat, mert ez a háttér esetleg hiányzik, de ún. részleges registry lockkal kínál nagyon biztonságos regisztrációt, az az ún. **INTEGRITY Védett Doménregisztráció**, mint szolgáltatás. Ez utóbbi szolgáltatás egy védelmi csomag, melynek különféle, akár mindegyik elem egyszerre is választható.

9.) Laikusként hogyan ellenőrizhetem legegyszerűbben, hogy a kapott e-mail feladója valóban az, aki küldte. Érvényes DKIM aláírás elegendő ehhez?

Sajnos önmagában a DKIM aláírás kevés.

Fontos leveleknél az ún. X.509-es tanúsítvány alapú SMIME email aláírás egyszerűbben kezelhető, vagy az, ha megfelelően digitálisan aláírt a levélben mellékelt dokumentum.

Laikusoknak gyakran képezniük kell magukat, hogy ne legyen teljesen laikusok. Egyszerű dolgokról van szó, melyet általános iskolában már oktathatnának, de sajnos még középiskoláknak sem reguláris tananyaguk.

Laikus számára megoldás a visszakérdezés: küld egy levelet a feladó email címére és visszakérdez, hogy valóban a feladó küldte. Ez egyszerű megoldás, csak sajnos egy plusz levélváltást igényel.

A DKIM-et, ha megismerjük, akkor sok esetben segíthet abban, hogy bizonyosabbak legyünk segítségével, hogy ki a feladó. Ha nem ismerjük kellően az Internet elektronikus levelezés és a DKIM működését, akkor viszont könnyen téves következtetésre juthatunk.

A DKIM-mel aláírt fogadott levelek értékelését inkább professzionális felhasználók számára ajánljuk, pl. megfelelően felkészített ügyfélszolgálat számára. Laikusok számára a visszakérdés általában a biztonságosabb.

Megjegyezzük, hogy akárcsak emailnél, postai levélnél se tudhatjuk általában a borítékról, hogy azt ki küldte. Ha telefonon hívnak, a kijelzett szám is lehet akár hamis, vagy csak egyszerűen nem a hívó telefonszáma. Telefonnál is, akár csak emailen, egy visszakérdezés, telefon esetében ez az adott telefonszám visszahívását jelenti, segít eldönteni a hívó kilétét. Mindig gondoljunk csak a postai levélre, és arra, hogy ellenőrizhetjük, hogy azt valóban a feladó küldte. Ugyanígy gondolkozzunk emailek esetén is!

10.) A DNSSEC mivel nyújt nagyobb védelmet a számomra?

A DNSSEC tudja azt biztosítani, hogy ne hamisíthassák meg a névszervert,
vagy ne tudják megbabrálni a névszerver és kliensünk közti forgalmat.

DNSSEC híján sajnos nem tudhatjuk, hogy nem történt-e visszaélés, a DNS szolgáltatta adatok azok valódiak-e.

Nem kritikus domének esetén a DNSSEC kevésbé fontos. Pl. a Wikipedia.hu nem alkalmaz DNSSEC-et. Ez bár helytelen szerintünk, végül is mi történik, ha meghamisítják a Wikipedia DNS-ét, valószínűleg semmi nagy baj, esetleg sikerül megtéveszteni bennünket, hogy a Mohácsi csatára keresve, az nem 1526-ban, hanem a családd hamisító közlése szerint 100 évvel korábban történt :-) Bár attól tartunk ennél sokkal csúnyább átverésre is el lehetne követné még a magyar Wikipédián is. Azonban egy nagy szolgáltató, webáruház, online banki fizető oldal stb. esetén a DNSSEC nem alkalmazása abszolút elfogadhatatlan.

Analyzing DNSSEC problems for wikipedia.hu

.	✓ Found 2 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
hu	✓ Found 2 DS records for hu in the . zone ✓ DS=2104/SHA-256 has algorithm RSASHA256 ✓ DS=20056/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=26116 and DNSKEY=26116 verifies the DS RRset ✓ Found 3 DNSKEY records for hu ✓ DS=2104/SHA-256 verifies DNSKEY=2104/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=2104 and DNSKEY=2104/SEP verifies the DNSKEY RRset
wikipedia.hu	✗ No DS records found for wikipedia.hu in the hu zone ✗ No DNSKEY records found ✓ wikipedia.hu A RR has value 91.146.180.88 ✗ No RRSIGs found

2020. november 25. 21.46, DNSSEC nem alkalmazott.

Megdöbentőbb, hogy a Wikipedia.com sem alkalmaz DNSSEC-et:

Analyzing DNSSEC problems for wikipedia.com

.	✓ Found 2 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
com	✓ Found 1 DS records for com in the . zone ✓ DS=30909/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=26116 and DNSKEY=26116 verifies the DS RRset ✓ Found 2 DNSKEY records for com ✓ DS=30909/SHA-256 verifies DNSKEY=30909/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
wikipedia.com	✗ No DS records found for wikipedia.com in the com zone ✗ No DNSKEY records found ✓ wikipedia.com A RR has value 208.80.154.232 ✗ No RRSIGs found

2020. november 25. 21.46, DNSSEC nem alkalmazott.

Nemigazán értjük, de valamiért a magyar bankok is ódzkodnak DNSSEC alkalmazástól, pl.:

Analyzing DNSSEC problems for otpbank.hu

.	✓ Found 2 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
hu	✓ Found 2 DS records for hu in the . zone ✓ DS=2104/SHA-256 has algorithm RSASHA256 ✓ DS=20056/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=26116 and DNSKEY=26116 verifies the DS RRset ✓ Found 3 DNSKEY records for hu ✓ DS=2104/SHA-256 verifies DNSKEY=2104/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=2104 and DNSKEY=2104/SEP verifies the DNSKEY RRset
otpbank.hu	✗ No DS records found for otpbank.hu in the hu zone ✗ No DNSKEY records found ✓ otpbank.hu A RR has value 195.228.112.250 ✗ No RRSIGs found

2020. november 25. 21.46, DNSSEC nem alkalmazott.

Természetesen, ha kár ér bennünket, mint banki ügyfelet, mert bankunk nem alkalmazott DNSSEC-et, akkor ezért a bank teljes felelősséggel tartozik, a kárunkat meg kell téríteni, hiszen **az várható el, hogy szolgáltatónk alkalmazzon DNSSEC-et**.

11.) Szolgáltatóm DNS szerverei egyben webszerverek is. Helyes-e ez?

Nagyon nem helyes!

Hacsak nem valami tesztkiszolgálásról van szó, akkor DNS szervereknek dedikált DNS szervereknek kellene lenni, semmilyen más szolgáltatást, pl. web- vagy e-mail szolgáltatást nem szabadna nyújtaniuk.

Mind biztonsági, mind elérhetőségi, rendelkezésre-állási és megbízhatósági szempontjából fontos a dedikált DNS szerverek alkalmazása, és ezen belül ez különösen fontos DoS/DDoS védelmi szempontból.

Még nem kritikus domének esetén sem javasolt ez a megoldás, mert biztonsági szempontból sérülékenyebb, mint dedikált DNS szervert alkalmazni.

12.) Szolgáltatóm csak két névszervert alkalmaz. Elégséges-e ez?

Először is érdemes ellenőrizni, hogy valóban csak két névszerver van, vagy anycast DNS szolgáltatás alkalmazott és valójában több névszerver is alkalmazott.

Két névszerver nem kritikus doménekhez elégséges, bár kérdés, hogy a szolgáltató miért nem alkalmaz többet?!

Ha több névszerver alkalmazott, akkor fontos kérdés, hogy milyen azok sávszélessége, kiszolgáló-teljesítménye, szoftver háttere, ugyanis egy szolgáltató szolgáltatása, mely több névszervert alkalmaz nem szükségképpen jobb egy másik csak két névszervert alkalmazó szolgáltatónál, de a névszerverek száma mégis egy fontos mutató, már csak azért is, mert ez viszonylag könnyen kikalkulálható mutató.

Jobb DNS szolgáltatások több tucat névszervert vagy akár száz feletti számút alkalmaznak (root névszerverek száma 1000 feletti).

Valójában a névszerverek száma csak egy mutató, egy szolgáltatás minősége ennél összetettebb. Kritikus doménnevekhez mindenesetre nem luxus több névszervert, illetve anycast szolgáltatást alkalmazni.

Gyakran a csak két névszerver arra utal, hogy a szolgáltató számára a DNS-szolgáltatás egy elhanyagolt terület, egy kényelmetlenség, melyet mellékesen, de nem professzionálisan szolgáltat. Érdemes megnézni pár további jellemzőt a szolgáltatás kapcsán, és ez megerősítheti gyanúnkat, hogy a szolgáltató csak mellékesen, 'ahogy van' ('as is') szinten nyújt DNS szolgáltatást.
Például gyanús,

- ha névszervernek lekérdezhető a szoftver típusa és verziója,
- ha worldwide szinten válaszidejük ingadozó vagy nagy,
- és nagyon nem jó jel, ha DNSSEC nem támogatott, de kritikus doménnevünkhöz bizonyára akarunk is DNSSEC-et alkalmazni.

Az IANA ajánlás minimum 2 névszervert ír elő követelményként, de ez a minimum, nem ez az ajánlott. Mint látható egyre kevesebb ügyfél és szolgáltató elégszik meg csupán 2 névszerverrel.

INTEGRITY Kft. szolgáltatásaival kapcsolatos kérdések

1.) Mit biztosít az INTEGRITY Kft. névszerver szolgáltatás alatt?

Az INTEGRITY nyújt **resolver** névszerver-szolgáltatást, de csak hoszting ügyfeleinek,

és nyújt **authoritatív** névszerver-szolgáltatást.

Az authoritatív névszerver-szolgáltatás céljára az ún. Standard és az ún. Prémium DNS szolgáltatást kínáljuk,
a **Standard** díjmentes az INTEGRITY Kft-nél regisztrált és fenntartott domainnevekhez,
a **Prémium** az valójában egy **szolgáltatáscsalád**, mely viszont díjfizetős,
illetve létezik egy legacy 'secondary only' DNS szolgáltatásunk is.

A Standard szolgáltatásban alapértelmezetten

- 3 unicast DNS szervert alkalmazunk,
- melyek egymástól függetlenül route-olt Internet kapcsolattal rendelkeznek,
- két földrajzi helyen kerültek elhelyezésre,
- adatbázis-alapú master-slave konfigurációjú rendszert alkalmazunk;
- díj ellenében zónákhoz biztosítunk egy 4. névszervert, melynek hálózati kapcsolata független az előzőektől.

2.) Hogyan biztosítja az az INTEGRITY Kft., hogy illetéktelen ne kérhessen jogosulatlan DNS szintű módosítást a domainnevem esetén?

A Prémium DNS szolgáltatásunk keretében igen sokféle biztonsági megoldást alkalmazunk,
a Standard DNS esetén az ügyfeleink jelszó védett weboldalon keresztül szerkeszthetik zónájukat (a webes felület szoftverét lényegi változtatások esetén auditáltatjuk).

Ügyfeleink, illetve ügyfeleink felhasználói kérhetnek egyrészt új jelszót, másrészt kérhetik azt, hogy ügyfélszolgálatunk módosítson zónát. Ilyen kérés esetén a jogosultságot manuálisan ellenőrizzük vissza, alapvetően az e-mail címet ellenőrizzük, ha a felhasználónk nem alkalmaz digitalis aláírást, akkor e-mail visszakérdezést alkalmazunk (de alkalmazhatunk erősebb authentikációt, akár többfaktoros authentikációt, de ezek már a Standard DNS szolgáltás esetén már díjfizetős jellemzők lehetnek).

Kritikus domainnevekhez, illetve zónákhoz a Prémium DNS szolgáltatást javasoljuk, itt többfaktoros authentikáció, API elérés vagy kliens rejtett DNS szerverről történő módosítás lehetséges, valamint IP korlát és/vagy VPN is alkalmazott.

Lehetőség van arra, hogy csak több személy együttes kérését teljesítsük, illetve a teljesítést több jogosult is letilthassa.

Kritikus domainekhez egyedi javaslatot teszünk az ügyfelünk igényeinek felmérése után, és egy Prémium DNS szolgáltatáscsomagot javaslunk, mely javaslat már az egyedi igényekre van testre szabva.