DNSSEC

Alapértelmezésben a domain nevek DNS bejegyzései egy egyszerű lekérdezés során nincsenek titkosítva, ezért illetéktelenek hozzáférhetnek, és módosíthatják a választ. A DNSSEC egy kriptográfiai eljárás segítségével írja alá a domain nevek zónáját, így hiteles választ fog vissza adni, amelyhez harmadik fél nem tud hozzáférni, nem tudja módosítani azt.

> A domain névnél helytelen DNSSEC beállítások használata a domain név működésképtelenségéhez vezethet.

MI A DNSSEC?

A DNSSEC a Domain Name System Security Extensions szavak rövidítéséből áll. Lényegében a DNS egy kiterjesztése amely a DNS megalkotása során keletkezett biztonsági hibákat, sebezhetőségeket hivatott javítani.

A DNSSEC MŰKÖDÉSE

A DNSSEC az adatok meghamisítása ellen védekezik olyan módon, hogy a DNS rekordokhoz digitális aláírást ad hozzá a lekérdezések során. A DNSSEC-el aláírt domain nevek zónáinak lekérdezése során a digitális aláírás – amelyet a domain névnél beállított névszerverben tárolnak – hitelesítésre kerül így biztosítva azt, hogy a lekérdezés és a válasz közötti időszakban a zónában tárolt adatok nem módosultak. A DNSSEC segítségével biztosítható hogy ténylegesen annak a weboldalnak a lekérdezése történjen meg amelyet a látogató a böngészője címsorába beírt.

A DNSSEC működését tekintve a nyílvános, illetve titkos kulcsú hitelesítést használja. A nyilvános kulcsokat digitális aláírásokat a DNS-ben RRSIG típusként lehet megtalálni, ezen rekordok ugyanúgy kérdezhetőek le mint bármely másik típusú rekord. A domain nevekhez tartozó titkos kulcsokat a névszerver tárolja, és egy lekérdezés során a titkos kulcs segítségével aláírt adatokat is vissza küldi a kérdező félnek, aki a nyilvános kulcs segítségével tudja feloldani ezt. Abban az esetben ha harmadik fél beleavatkozik a lekérdezésbe és módosítja a válaszban elküldött adatot, akkor a visszafejtés során a nyilvános kulcs segítségével nem lehet majd helyesen vissza fejteni azt, ebből viszont tudni fogja a fogadó fél, hogy azt meghamisították.

A DNSSEC nem végez adat titkosítást – algoritmusok hiányában -, csak azt biztosítja, hogy a lekérdezett adatok eredetiek. Ebből adódóan a DNSSEC-et nem lehet használni például DDoS támadás kivédésére.

DNSSEC KULCS KEZELÉS

Természetesen mint minden kriptográfiai eljárást a DNSSEC esetében használt privát és nyílt kulcsok is megismerhetőek, és feltörhetőek idővel. Azért hogy a használt kulcsokat nehezebben lehessen megismerni és ezt követően feltörni, bevezetésre került egy plusz kulcs. A DNSSEC esetében a KSK, és a ZSK típusú kulcsok vannak használatban. A KSK kulcsok viszonylag ritkán változnak, azonban a ZSK kulcsok gyakran, így biztosítva azt hogy egy esetleges feltörés sokkal időigényesebb, és ez által nehézkesebb legyen.

Kulcs fajtája	Kulcs leírása
KSK	ennek segítségével írják alá a zóna aláíró kulcsot
ZSK	ennek segítségével kerülnek aláírásra az egyes rekordok

DNSSEC ENGEDÉLYEZÉSE

Abban az esetben ha a domain név az alapértelmezett, vagy a cPaneles tárhely által biztosított névszervereket használja akkor a DNSSEC bekapcsolása az alábbi módon kapcsolható be:

1. A bejelentkezést követően a felső menü sorban kattintson a **Domainek** / **Domain neveim** menü pontra.
2. A jobb oldalon felül található keresőben rá tud keresni a domain névre, ha a domain nevet megtalálta akkor kattintson a **Domain kezelése** menü pontra.
3. A megjelenő oldalon kattintson a **DNSSEC** lehetőségre.
4. Abban az esetben ha a domain névnél nem volt korábban engedélyezve a **DNSSEC** akkor azt a **DNSSEC engedélyezése** gombra történő kattintással engedélyezheti.

DNSSEC HIBAELHÁRÍTÁSA

Az alábbi oldalak segítségével ellenőrizhető a DNSSEC helyes beállítása:

- Verisign DNSSEC Debugger
- DNSViz

Változat #1
DotRoll Tudásbázis hozta létre 2023-09-20 11:46:22 CEST
DotRoll Tudásbázis frissítette 2023-09-20 11:47:50 CEST