DOM REG [.lt]

DNS autoritatyvių serverių administravimo gerosios praktikos pavyzdžiai

Tomas Simonaitis, Mantas Gavėnas

KTU IPC

Kaunas, 2023-12-05

DNS autoritatyvių DNS serverių PĮ

- *Bind9 (rekursinis ir autoritatyvus)*
- *NSD (tik autoritatyvus)*
- *Knot DNS (tik autoritatyvus)*
- *Yadifa (tik autoritatyvus)*
- *PowerDNS Authorative Server*

DOM REG [.lt]

Pagrindinės gerosios praktikos

- *Leisti UDP/53 užklausas iš visų IP*
- *Leisti **TCP/53** užklausas iš visų IP*
- *Domeną turėtų aptarnauti bent du (**2**) DNS serveriai*
- *Atskirti rekursinius ir autoritatyvius serverius*

DOM REG [.lt]

Antras DNS serveris

- *Jei administruojate tik vieną DNS serverį, .lt domenams galite neatlygintinai naudoti ns2.domreg.lt*

Neleiskite zonos nukrovimo (AXFR) pašaliniams

- *DNS zonas leiskite nusikrauti tik savo DNS serveriams*

DOM REG [.lt]

Neleiskite zonos nukrovimo (AXFR) pašaliniams

- *Bind9: allow-transfer*
- *NSD: provide-axfr*
- *Knot DNS: action: transfer*

DOM REG [.lt]

Užtikrinkite zonos nukrovimo autentiškumą

- *TSIG (vienodas pre-shared key tarp jūsų autoritatyvių serverių)*
- *XoT (AXFR over TLS)*

DOM REG [.lt]

Neprivalote aptarnauti ANY užklausų

- *ANY užklausos praktikoje naudojamos retai, bet dažnai siunčiamos amplifikacijos atakose (maža užklausa – didelis atsakymas)*

DOM REG [.lt]

Neprivalote aptarnauti ANY užklausų

- *Bind9: minimal-any yes*
- *NSD: refuse-any yes*
- *Knot DNS: disable-any on*

DOM REG [.lt]

Ribokite atsakymų srautą

- *Jūsų serveriams siunčiamos UDP užklausos su padirbtu šaltinio adresu gali būti naudojamos amplifikacijos atakoms*

DOM REG [.lt]

Ribokite atsakymų srautą

- *Bind9: rate-limit*
- *NSD: rrl-ratelimit*
- *Knot DNS: mod-rrl*

DOM REG [.lt]

Stebėkite DNS serverių veikimą

- *... ar DNS serveris veikia*
- *... kiek užklausų aptarnauja*
- *... ar grąžina SERVFAIL atsakymų*

DOM REG [.lt]

Stebėkite DNS serverių veikimą

- *Bind9: rndc status*
- *NSD: nsd-control stats_noreset*
- *Knot DNS: knotc stats*

DOM REG [.lt]

AČIŪ

- https://kindns.org
- https://zonemaster.iis.se
- https://dnsviz.net
- https://dnssec-analyzer.verisignlabs.com/

DOM REG [.lt]