

DNS filtravimas – saugus internetas jūsų verslui

Kas yra DNS filtravimas?

DNS filtravimas – tai paslauga, leidžianti kontroliuoti, kokias svetaines galima pasiekti per jūsų įmonės tinklą. Naudodami DNS (Domenų Vardų Sistemos) užklausų valdymą, užtikriname, kad jūsų darbuotojai galėtų prisijungti tik prie patikimų ir saugių svetainių.

Kaip tai veikia paprastai?

Kai naršyklėje įvedate svetainės adresą, DNS filtravimo sistema patikrina, ar ta svetainė yra patikima. Jei svetainė įtraukta į kenksmingų sąrašą (pvz., kenkėjiškos, apgaulingos, sukčiavimo ar nesaugių turinio svetainės), prisijungimas prie jos blokuojamas. Taip jūsų tinklas apsaugomas nuo grėsmių.

Kodėl jūsų įmonei reikia DNS filtravimo?

Apsauga nuo kibernetinių grėsmių: Blokuojame prieigą prie žinomų kenksmingų svetainių, užkertant kelią kenkėjiškoms programoms, virusams ir sukčiavimui.

Darbo produktyvumo užtikrinimas: Ribojame prieigą prie svetainių, kurios trukdo darbui, pavyzdžiui, socialinių tinklų ar žaidimų puslapių, pagal jūsų nustatytą politiką.

Atitiktis saugumo standartams: DNS filtravimas padeda įgyvendinti organizacijos saugumo politiką ir atitikti reguliacinius reikalavimus.

Techninė informacija apie DNS filtravimą

DNS filtravimo sistema veikia kaip tarpininkas tarp vartotojo ir interneto. Kai vartotojas siunčia DNS užklausą (pvz., įvesdamas svetainės adresą), sistema patikrina šią užklausą pagal iš anksto nustatytus filtravimo politikos taisykles. Jei svetainė neatitinka reikalavimų, užklausa yra blokuojama, o vartotojas gauna pranešimą apie užkardytą prieigą.

Atvirojo kodo sprendimai ir duomenų bazės

Mūsų DNS filtravimo paslauga yra pagrįsta patikimais atvirojo kodo sprendimais, tokiais kaip "Pi-hole" ar "Bind". Informaciją apie kenksmingus domenus gauname iš šių nemokamų ir patikimų duomenų bazių:

- ✓ Spamhaus: Dėl duomenų apie žinomus sukčiavimo ir kenkėjiškų svetainių adresus.
- ✓ OpenPhish: Fokusuojasi į sukčiavimo (phishing) svetainių aptikimą.
- ✓ Emerging Threats: Grėsmių duomenų bazė, apimanti naujausias kenkėjiškas svetaines.
- ✓ IBM X-Force Exchange: Platesnis grėsmių stebėjimas ir analizė.

- ✓ PhishTank: Bendruomenės valdoma svetainių, susijusių su sukčiavimu, duomenų bazė.

Papildomos techninės funkcijos

Realiuoju laiku atnaujinamos duomenų bazės: DNS filtravimo sistema automatiškai sinchronizuojasi su pasirinktų duomenų bazių atnaujinimais.

Kategorijų filtravimas: Svetainės filtruojamos pagal kategorijas (pvz., socialiniai tinklai, suaugusiųjų turinys, sukčiavimas), leidžiant įmonėms pritaikyti filtravimą pagal savo poreikius.

Caching mechanizmas: Užklausų spartinimui DNS sistema naudoja atsarginių kopijų saugojimą (caching), užtikrindama greitą atsaką į dažnai lankomus adresus.

Integracija su įmonės tinklu: DNS filtravimo sprendimas lengvai integruojamas su esama VPN sistema, užtikrinant, kad apsauga veiktų ir biure, ir nuotoliniu būdu.

Analitika ir stebėjimas: Platforma leidžia stebėti, kurios svetainės buvo blokuotos, ir analizuoti tinklo naudojimo tendencijas.

Kodėl verta rinktis mūsų DNS filtravimo paslaugą?

Saugumas be kompromisų: Užkertame kelią pavojingoms užklausoms dar prieš joms pasiekiant jūsų tinklą.

Lengvas valdymas: Vartotojui draugiška valdymo panelė leidžia greitai pritaikyti saugumo taisykles.

Visuotinė apsauga: Mūsų DNS filtravimas veikia tiek biuro aplinkoje, tiek nuotoliniu būdu dirbantiems darbuotojams.

Pavyzdys :

Įsivaizduokite: vienas jūsų darbuotojas netyčia paspaudžia ant el. laiško nuorodos, kuri veda į apgaulingą svetainę. Mūsų DNS filtravimo sistema automatiškai blokuoja prieigą prie šios svetainės, apsaugodama įmonės duomenis nuo vagystės ar kenkėjiškų programų.

Užtikrinkite, kad jūsų tinklas būtų apsaugotas ir tinkamai valdomas, rinkdamiesi mūsų DNS filtravimo paslaugą. Tai sprendimas, kuris dirba tyliai, bet efektyviai, saugodamas jūsų įmonės veiklą kiekvieną dieną.