.LV

REĢISTRATŪRU AVĪZE

2020
#9
www.nic.lv

ŠAJĀ NUMURĀ LASIET:

INOVĀCIJU APREIBINĀTIE PIEMIRST PAR DROŠĪBU

Pēdējo desmit gadu laikā jauni tehnoloģiju sasniegumi ir ieplūduši tirgū kā viesulis, tas ir ietekmējis arī mūsu mijiedarbību ar digitālo pasauli. Internets ir kļuvis daudz ātrāks un mobilāks nekā jebkad agrāk - varam piekļūt tam, izmantojot savu pulksteni vai mākslīgo intelektu (AI), kas atpazīst mūsu balsis. Varam pat mijiedarboties ar to, izmantojot virtuālo un paplašināto realitāti (AR), izkliedējot līnijas starp to, kas ir īsts, un to, kas digitāls. Vai spējat iedomāties, ka pirms 10 gadiem cilvēki pat nenojauta, kas ir "*selfie stiks*" (izgudrots 2014. gadā), neizmantoja *Instagram* (2010. gads), jaunieši tiešām savā starpā sarunājās, nevis sūtīja *SnapChat* (ieviests 2011. gadā) ziņas un iepazinās pasākumos, nevis tiešsaistē, izmantojot *Tinder* (2014. gads).

Tagad 2020. gadā mēs paļaujamies un uzticamies šīm lietotnēm, piemirstot, ka, lai gan šie jauninājumi padara mūsu sadzīvi ērtāku, tie arī ievērojami palielina digitālā privātuma un uzbrukumu risku. Ne velti viena no interneta lietotāju nozīmīgākajām bažām šodien ir personas datu uzraudzība un to dažkārt pat apšaubāmā izmantošana. Pareizi uzglabāti un apkopoti dati sniedz informāciju, kas maksā "miljonus". Ar tiem pēdējo gadu laikā ir veiksmīgi manipulējuši vairāki ievērojami uzņēmumi, kā *Facebook*, *Cambridge Analytica* un citi. Tādēļ viens no šīs avīzes rakstiem ir veltīts **digitālajam privātumam**, konkrēti DNS plūsmas šifrēšanai.

Pēdējo 10 gadu laikā ir pieredzēta arī ievērojama domēna vārdu telpas paplašināšanās. 2011. gadā ICANN atcēla lielāko daļu vispārējo augstākā līmeņa domēnu (gTLDs) izveides ierobežojumu. Šis lēmums izraisīja jaunu domēnu "sprādzienu" un sarakstam tika pievienoti vairāk nekā 1000 jaunu ICANN apstiprinātu gTLD (piemēram, .apple, .lawyer, .xyz, .sex, utt.). Ar jauno vispārējo augstākā līmeņa domēnu tirgus tendencēm Latvijā un Baltijā 2019. gadā varat iepazīties portāla pardomenu.lv rakstā šeit. Lai gan šo jauno gTLDs ieviešana sniedza daudz pozitīvu iespēju, tas ir ļāvis arī ļaundariem reģistrēt simtiem vai pat tūkstošiem domēna vārdu ar nolūku tos izmantot kiberuzbrukumos, piemēram, pikšķerēšanā vai smikšķerēšanā (uzbrukums izmantojot SMS vai citas ziņu sūtīšanas tehnoloģijas). Ļaundaru apkarošanu un identificēšanu neatviegloja 2018. gada maijā īstenotā ES Vispārīgā datu aizsardzības regula (VDAR), kas būtiski ietekmēja WHOIS publiski pieejamās informācijas apjomu. Ar aizgājušā 2019. gada karstākajām aktualitātēm domēnu industrijas pasaulē varat iepazīties mūsu avīzes 3.-4. lpp.

Ir grūti paredzēt, kas mūs sagaida 2030. gadā. Turpināsim vērot, kā tiek gudrotas un veidotas jaunas un aizraujošas tehnoloģijas, izmantojot mākslīgo intelektu (AI), *Machine Learning* un *Natural Language Processing*. Kā un vai inovācijas ietekmēs domēnu industriju vēl grūti spriest, taču paredzam, ka arī ļaundari negulēs rokas klēpī salikuši. Tādēļ DNS drošībai nākamajā desmitgadē tiks pievērsta liela vērība. Vai pieaugošā DNS ļaunprātīgā izmantošana mainīs arī domēnu reģistra uzturētāju un reģistratūru atbildību, vai palielināsies domēna vārdu bloķēt gribētāju pulks pasaulē un Latvijā?

Neatbildētu jautājumu ir daudz, tādēļ aicinām ikvienu sekot līdzi aktualitātēm un meklēt atbildes kopā, apmeklējot .LV, .LT un .EE rīkotās Baltic Domain Days (Baltijas Domēnu Dienas), kuras šogad norisināsies no 28. līdz 29. maijam Viļņā, LOGIN konferences ietvaros (www.login.lt). Uz tikšanos Baltijas Domēnu Dienās!

Ar cieņu,
Dana Ludviga
.LV reģistra (NIC)
PR un mārketinga daļas vadītāja

#BALTIC DOMAIN DAYS

PART OF

LOGIN x 28 - 29 MAY 2020 VILNIUS LITHUANIA

.LV, .EE un .LT domēnu reģistri aicina Jūs uz Baltijas valstu domēnu nozarei veltītu konferenci - Baltic Domain Days, kura šogad norisināsies tehnoloģiju un inovāciju festivāla LOGIN ietvaros Lietuvas izstāžu un konferenču centrā LITEXPO.

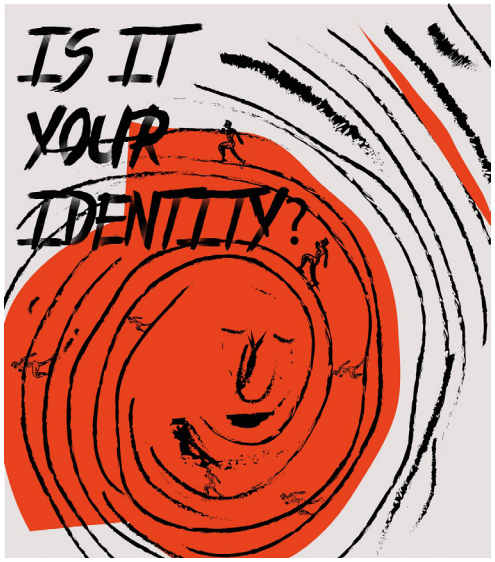
LOGIN ar saukli "Progress, inovācijas un tehnoloģijas" vairāk nekā 14 gadu tās pastāvēšanas laikā ir kļuvusi par lielāko šāda veida konferenci Baltijā, ik gadu pulcējot ap 4000 cilvēku. Tādēļ šogad Baltijas Domēnu Dienu ietvaros ir iespēja ne tikai salīdzināt un novērtēt Baltijas valstu pieredzi, diskutēt un veidot kontaktus ar vadošajiem Lietuvas, Igaunijas un Latvijas domēnu un interneta nozares pārstāvjiem, bet arī novērtēt inovāciju festivāla LOGIN uzaicināto IT speciālistu nākotnes attīstības redzējumu.

.LV Reģistratūrām tiks izsūtīti ielūgumi ar pasākuma bezmaksas reģistrācijas kodu. Detalizētāka informācija par pasākumu tiks publicēta www.nic.lv vai rakstot uz pr@nic.lv.

Konference norisināsies Lietuvas izstāžu un konferenču centrā LITEXPO – Laisves ave.5, Viļņā.

SVARĪGĀKAIS DOMĒNU VĀRDU PASAULĒ 2019. GADĀ

Domēnu vārdu sistēma tādā vai citādā veidā ietekmē ikvienu interneta lietotāju, pat ja viņš vai viņa šādu ietekmi nekad nav izjutis. Šajā rakstā aplūkosim dažus svarīgākos notikumus, ko domēnu vārdu pasaule intensīvi apsprieda 2019. gada laikā.



DROŠĪBA PIRMAJĀ VIETĀ

Kā vienmēr, domēnu vārdu sistēmas drošībai tika pievērsta pastiprināta uzmanība. 2019. gada 15. februārī ICANN (globālā interneta pārvaldības organizācija Internet Corporation for Assigned Names and Numbers jeb Interneta vārdu un numuru piešķires korporācija) publicēja brīdinājumu par notiekošajiem mēģinājumiem sagraut domēnu vārdu sistēmu. Lai arī neko sagraut nav izdevies, visiem reģistriem un reģistratūrām tika piekodināts rūpēties par drošību un arī rekomendēti pasākumi drošības stiprināšanai. Šie jautājumi tika arī regulāri apspriesti kārtējās globālā līmeņa ICANN konferencēs.

WHOIS VAIRĀK NEBŪS

Ļoti nopietns panākums ir RDAP protokola tehniskā ieviešana visos vispārējo augstāka līmeņa domēnu (gTLD) reģistros un reģistratūrās, kas tika pabeigta 26. augustā. RDAP (Registration Data Access Protocol) paredzēts kā aizvietotājs labi pazīstamajam WHOIS protokolam, kas tiek izmantots informācijas sniegšanā par domēnu vārdu reģistrētāju. RDAP nodrošinās informācijas sniegšanu, ievērojot ES skaļi izskanējušās regulas par vispārējo datu aizsardzību GDPR (General Data Protection Regulation) un citu valstu datu aizsardzības likumu prasības.

> **Jaunajā protokolā domēnu vārdu turētāju datu bāzi veidos strukturētāku, ar precīzākiem datu pieprasījumiem, labāku internacionālo domēnu vārdu (IDN) atbalstu un, pats galvenais, publiskā pieejā ļaus iegūt tikai pamatinformāciju. Tikai speciāli izvēlētas iestādes drīkstēs piekļūt pilnai informācijai.**

Kāda tieši informācija ir jāievāc no reģistrētāja un kā un kam nodrošināt piekļuvi šai informācijai, paātrinātā politikas izstrādes procesā jeb EPDP (Expedited Policy Development Process) apspriež speciāli izveidotās darba grupas. Procesa pirmās fāzes darba atskaite tika publicēta 2019. gadā, un pašlaik tiek apspriesta. Ieinteresētajām pusēm šī atskaite ir jāakceptē līdz 2020. gada 29. februārim. Paralēli norit darbs otrajā fāzē, ko turpina cita darba grupa, kurai ir jāizstrādā rekomendācijas sistēmai, kas nodrošinās piekļuvi pie datu bāzes informācijas – kas tieši var informāciju saņemt un kā. Šīs darba grupas vadītājs ir Jānis Kārkliņš, Latvijas sūtnis ANO Ženēvā, bijušais ICANN Padomes loceklis.

SKANDĀLS AR .ORG CENĀM UN PĀRDOŠANU

Lielu "šūmēšanos" interneta sabiedrībā izraisīja ICANN 30. jūnija jaunais līgums ar augstākā līmeņa domēna **.org** reģistra uzturētāju PIR (*Public Interest Registry*, kas pieder ISOC jeb Internet Society).

> **Jaunais līgums paredz, ka turpmāk vairs netiek uzlikti ierobežojumi reģistra uzturētāja cenu politikai. Iepriekšējais līgums, kura darbība beidzās 2019. gadā, saturēja noteikumu, ka cenas nedrīkst celt vairāk par 10% gadā.**

ICANN Valde pieņēma lēmumu atcelt cenu izmaiņu ierobežojumus jaunajā līgumā dēļ tā, lai nodrošinātu vienādus noteikumus visiem vispārējiem augstākā līmeņa domēniem (gTLD), jo jaunie gTLD, kuri tiek ieviesti pēc 2013. gada, domēna vārdu reģistrācijas cenu var noteikt brīvi, nesaskaņojot to ar ICANN. Piemēram, par domēna vārda reģistrēšanu domēnā **.bank** var nākties šķirties no vairāk nekā 1000 eiro. Tiesa gan, pat šāda summa nav nekas briesmīgs tiem, kam interesē domēnu vārdi ar **.bank** beigās. Bet TLD **.org** tika radīts, lai tur varētu reģistrēties dažādas organizācijas – arī nekomerciālās un bezpeļņas biedrības, kam tomēr nauda ir jāskaita.

> **Nevienam nepatīk cenu kāpums, bet interneta sabiedrība izteica arī nopietnākas bažas par cenu ierobežošanas atcelšanu. Ja nu tagad cenas par domēnu vārdu reģistrēšanu un uzturēšanu krietni uzkāpj, tad daudzas bezpeļņas organizācijas var būt spiestas atteikties no savu mājaslapu veidošanas vai arī slēgt jau esošās, kas jau izskatās pēc brīvības ierobežošanas.**

Bet, ja kāda organizācija atsakās no domēna vārda domēnā **.org** un sameklē sev lētāku variantu, piemēram, **.lv**, tad, nerunājot par nepieciešamību informēt sabiedrību par jauno adresi, veco domēnu vārdu no **.org** var nopirkt kāds ļaundaris un krietni sarežģīt dzīvi šai organizācijai.

Sašutums par šo lēmumu vēl vairāk pieauga, kad novembrī kļuva zināms, ISOC vēlas pārdot **.org** reģistra uzturētāja kompāniju *Public Interest Registry* (PIR) kompānijai Ethos Capital par 1,135 miljardiem dolāru. Rezultātā PIR zaudētu savu līdzšinējo bezpeļņas organizācijas statusu un par savu galveno mērķi izvirzītu peļņas gūšanu. Lietai sevišķu pikantumu piešķir fakts, ka kompānijā *Ethos Capital* kā konsultants piestrādā *Fadi Chehadé*, bijušais ICANN organizācijas vadītājs (2012-2016).

Patiesības labad jāpiezīmē, ka augstas PIR un *Ethos Capital* amatpersonas regulāri uzstājas ar apgalvojumiem, ka nekāds cenu pieaugums nav paredzēts un nebūs. Šie paziņojumi, lai cik godprātīgi tie arī būtu, nevienu nepārliecina, jo gan PIR, gan Ethos Capital vēlāk var tikt pārdots tālāk, un jaunie īpašnieki nekā nebūs solījuši un varēs cenas paaugstināt pēc sirds patikas. PIR pārdošana bija nepatīkams pārsteigums arī ICANN, kas varētu atkārtoti izvērtēt savu lēmumu noņemt cenu ierobežojumu. Tāpēc cīņa par domēna **.org** cenām vēl nav galā.

Nākamais rindā ir .com domēns. Esošais līgums ar kompāniju Verisign Inc. par domēna .com uzturēšanu ar cenu augšanas ierobežojumiem beidz savu darbību 2024. gadā. Tad var gaidīt, ka jaunais līgums neparedzēs esošo cenas celšanas ierobežojumu saglabāšanu un pašreizējā cena par .com domēna vārdiem, kas ir ap 10 dolāriem, celsies. Verisign jau ir privāta kompānija, un tā uztur ap 160 miljoniem .com domēna vārdu.

JAUNIE AUGSTĀKĀ LĪMEŅA DOMĒNU VĀRDI

Kaut arī ir pagājuši jau 8 gadi kopš sākās jauno vispārējo augstākā līmeņa domēnu (gTLD) ieviešana, tā tomēr turpinājās vēl arī 2019. gadā. Īpašs notikums bija gTLD **.music** veiksmīga izsole aprīlī, kurā negaidīti uzvarēja kompānija DotMusic Ltd. Šī kompānija ir bāzēta Kiprā, un tur to balsta viena no lielākajām nekustāmā īpašuma kompānijām. Bet, protams, šai kompānijai ir daudz mazāk naudas nekā tādiem šīs izsoles dalībniekiem kā Amazon vai Twitter (pavisam bija 8 dalībnieki). DotMusic īpašnieks Konstantins Rusos, kurš pats arī ir mūziķis, ar ideju par šādu gTLD sāka aizrauties jau 2005. gadā, kad vēl tikai sākās runas par jaunajiem gTLD. Viņš arī meklēja un ieguva lielu atbalstu muzikantu vidē, bet tam nevarēja būt liela nozīme izsolē, kur jānosauc naudas summas. Cik daudz tika nosolīts par šo domēnu, netiek atklāts.

Ilgie pretendentu strīdi pa to, kuram visvairāk pienākas .music domēns, kavēja arī domēna .gay piešķiršanu, kas beidzot notika 2019.g. martā.

Te izsolē sacentās četri pretendenti un uzvarēja kompānija Top Level Design, kura parakstīja attiecīgo līgumu ar ICANN 23. maijā. Šī kompānija tika speciāli dibināta 2012. gadā jauno gTLD pārvaldībai un tagad uztur domēnu **.design** (vispopulārākais), **.ink** un **.wiki** reģistrus. Kad sāksies domēnu vārdu piešķiršana jauniegūtajā augstākā līmeņa domēnā .gay, nav droši zināms. Iespējams, ka 2020. gada maijā.

Strīds par gTLD .AMAZON turpinājās arī visu 2019.gadu. Amazones baseina valstis iebilst pret šī domēna piešķiršanu kompānijai Amazon.com, Inc. (jā, tieši tāds ir šīs kompānijas oficiālais nosaukums).

Vēl novembrī ICANN konferencē Monreālā tika izskatīti Kolumbijas iebildumi, bet nekāds lēmums netika pieņemts. Tagad, kad jau kādu laiku apspriež nākamo augstākā līmeņa domēnu ieviešanas posmu, kavēšanās ar pirmā posma domēnu atvēršanu ir diezgan nevēlama.

.music

DOMĒNU VĀRDU CENAS REKORDS

Vēl par domēnu vārdiem var piebilst, ka 2019. gadā tika uzstādīts jauns domēna vārdu cenas rekords.

Kompānija *Block.one* nopirka domēna vārdu Voice.com no kompānijas *Microstrategy* par 30 miljoniem dolāru.

Viens no iepriekšējiem rekordiem piederēja domēna vārdam Sex.com, kas tika pārdots par 13 miljoniem. Tā gan ir tikai zināmā cena, bet ne vienmēr cenas tiek izpaustas. Iespējams, kaut kur kāds domēna vārds arī bija dārgāks par 13 miljoniem.

Kompānija *Block.one* nodarbojas ar blokķēžu biznesu un ieņēmumus rēķina miljardos. Tā tā ir paredzējusi izmantot voice.com tāda sociālā tīkla veidošanai, kurš būtu bāzēts uz blokķēžu tehnoloģijas un tāpēc daudz drošāks pret privātās informācijas noplūšanu.

Domēnam jau var pieslēgties, kaut kas tur tiek darīts, un tīkla beta versiju paredzēts palaist 2020. gada 14. februārī. Acīmredzot kompānijas sapnis ir izkonkurēt Facebook. Redzēs, vai izdosies, jo viņi nav vienīgie ar šādu sapni.

1. Informācija par voice.com iegādi.
2. Informācija par RDAP.

DNS ŠIFRĒŠANA AR DOH UN DOT

Kad bažas par datu uzraudzību un tā apšaubāmu izmantošanu tikai pieaug, DIGITĀLAIS PRIVĀTUMS kļūst arvien nozīmīgāks. Jau 2018. gadā tādi ievērojami IT nozares uzņēmumi, kā Google, Mozilla un CloudFlare, izziņoja plānu turpmāk DNS trafiku šifrēt. Arī mēs NIC ejam laikam līdzi un kopš 2019. gada piedāvājam iespēju šifrēt DNS datu plūsmu (ar DoH vai DoT), izmantojot NIC DNS rekursīvo serveri.

Domēna vārdu sistēma (DNS - Domain Name System) ir interneta pamata protokols, kas darbojas kā liela datubāze vai tulks, pārveidojot cilvēkiem viegli saprotamās vārdiskās resursu adreses uz datoriem saprotamām skaitliskajām (IP) adresēm.

> **Problēma ar šo komunikāciju ir tā, ka DNS darbojas atklātā teksta (plain text) režīmā, proti, jebkurš pasīvs tīkla vērotājs var apskatīt pieprasījumu paketes un noskaidrot, kādas tīmekļa vietnes un resursus tu vai tavi kolēģi esat iecienījuši apmeklēt. Ja kāds vēlētos šos datus apkopot un analizēt, tas varētu iegūt unikālu informāciju par mūsu paradumiem, interesēm un vajadzībām.**

Daļai cilvēku var likties, ka tas nav nekas īpašs, jo “Man taču nav ko slēpt”. Tomēr var pienākt mirklis ikkatra cilvēka dzīvē, kad dažas lietas mēs vēlamies paturēt tikai pie sevis. Vai jūs nemulsinātu fakts, ka kāds jūsu tīkla vērotājs var redzēt, ka apmeklējat anonīmo alkoholiķu, vēža vai AIDS pacientu atbalsta portālus, vai, piemēram, depresijas vai sieviešu atbalsta grupu tīmekļa vietnes? Jā, arī tik sensitīva informācija ir iegūstama vienkārši, apskatot jūsu DNS datu plūsmu.

Ar šo informāciju var manipulēt un izmantot, lai apkopotu un veidotu galalietotāju profilus, kurus parasti izmanto mērķētai mārketinga materiālu vai viltus ziņu izplatīšanai un konkurences analizēšanai. Piemēram, Facebook, “acīmredzamās” datu privātuma vienaldzības dēļ, vairāku gadu garumā ir apkopojis lietotāju datus mērķētu reklāmas kampaņu, jo īpaši politisko reklāmu, izplatīšanai. Tas nav maznozīmīgi, jo šīs kampaņas ir guvušas lielus panākumus. Visziņkārākais likumpārkāpējs šajā jomā ir politiskā konsultāciju un stratēģiskās komunikācijas firma *Cambridge Analytica*, kas, izmantojot *Facebook* lietotāju personu datus, veiksmīgi vadīja “Pro Brexit Leave” un Donalda Trampa 2016. gada prezidenta vēlēšanas kampaņas.

> **Datu konfidencialitāte ir kļuvusi par sabiedrības rūpi mūsdienu digitālajā laikmetā. Ikvienam būtu jāpievērš uzmanība un jārūpējas par savu datu privātumu, kā arī jāzina, kā tos aizsargāt.**

Par laimi ir novērojama ar vien lielāka sabiedrības interese par digitālo privātumu. Interneta lietotāji sevi izglīto šajos jautājumos, akli nepaļaujoties, ka Vispārīgā datu aizsardzības regula (VDAR) vai kāds cits datu aizsardzības likums sargās viņu datus, jo *likumi taču ietekmē tikai likuma paklausīgus pilsoņus un uzņēmumus*.

DNS datu šifrēšana nodrošina datu konfidencialitāti, tādēļ ir raisījusi lielu sabiedrības interesi. Vieni testē un meklē nepilnības, vai strīdas, kurš no risinājumiem DoH vai DoT ir labāks. Savukārt citi priecājas, ka beidzot šī tēma tiek aktualizēta, un paši var izvēlēties, kura izstrādātāja DNS serveri izmantot savas datu plūsmas šifrēšanai. Taču, ja arvien vairāk interneta lietotāju steigsies izmantot dažu lielāko uzņēmumu DNS serverus, vai neiekritīsim citā slazdā? Kur garantija, ka šo uzņēmumu vērtības laika gaitā nemainīsies un neradīsies vēlme monetizēt iegūto informāciju?

MAZLIET PAR DOH & DOT ATŠĶIRĪBĀM

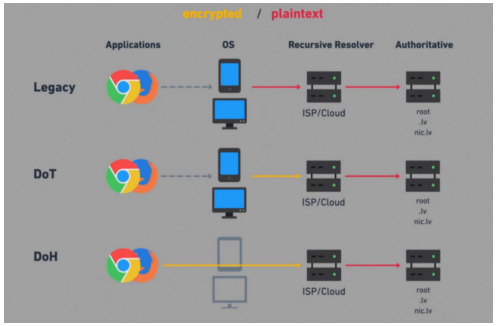
Ir divas alternatīvas, kā šifrēt DNS datu plūsmu starp DNS klientu un DNS serveri - **DNS over TLS** (*Transport Layer Security*) jeb **DoT** un **DNS over HTTPS** jeb **DoH**. Abiem protokoliem pastāv nozīmīgas atšķirības, dažas no tām šajā rakstā apskatīsim.

DoT ir IETF RFC 7858 standarts, kas nodrošina plūsmas šifrēšanu visai OS, nevis konkrētai aplikācijai, kā to dara DoH. DoT izmanto TCP kā pamata savienojuma protokolu un TLS priekš šifrēšanas un autentifikācijas. Savukārt DoH, lai izveidotu savienojumu, izmanto HTTPS un HTTPS 2. Tā ir svarīga atšķirība, jo ietekmē, kurš no portiem tiek lietots. DoT ir savs ports – 853 (šis ports ugunsmūros būs jāatver), bet DoH izmanto 443 portu, kas ir standarta ports HTTPS trafikam. DoH (RFC 8484) ir program-

matūras pusē ieviesta šifrēšana. Šifrētā DNS rezolūcija notiek tikai no noteiktās aplikācijas, kurā tā ir uzstādīta. Proti, ja DoH tiek uzstādīts *Firefox*, tad tikai *Firefox* to izmantos. Svarīgi zināt, ka šī aplikācija apies jau OS uzstādīto DNS serveri, proti, runās tieši ar to NS, kuru uzstādījis programmatūras vai aplikācijas izstrādātājs, kas var radīt dažas problēmas:

- **Iespējama interneta plūsmas koncentrācija** — ja tīmekļa pārlūka programmatūras izstrādātājs ieviešnoklusējuma (default) vērtības, kas norāda uz konkrētu interneta pakalpojumu sniedzēja (IPS) DNS serveriem, tad visa interneta plūsma nokļūst viena IPS rokās.
- **Drošības filtru ignorēšana** — ja uzņēmums ir uzstādījis iekšējos drošības aizsardzības mehānismus un filtrēšanu, izmantojot DNS ugunsmūri, tie var tikt apieti. Tiks ignorēti /etc/hosts, ja izmantojat *Linux*, *Windows* gadījumā - hosts failā norādītie uzstādījumi.
- **Iekšējo resursu nepieejamība** — uzņēmumi, kuri izmanto iekšējos domēnus vai atdalītus domēnu uzstādījumus ar piekļuvi iekšējā tīkla resursiem, var saskarties ar problēmām. Ja jūsu OS lokālais DNS serveris tiek apiets, pārlūkprogramma vienkārši nespēs attēlot uzņēmuma iekšējos resursus.
- **Satura piegādes tīkla (*CDN - Content Delivery Network*) "muļķošana"** – daudzu CDN darbība ir DNS bāzēta, tādēļ, ja izmantojat izstrādātāja DoH, kurš atrodas tālu no Latvijas, CDN uzskatīs, ka atrodaties citā valstī (pieņemsim Amerikā). Tas ietekmēs, piemēram, video straumēšanas ātrumu, to augšupielādējot no ASV serveriem.

Kā redzams attēlā, abi no šiem protokoliem šifrē tikai daļu no DNS pieprasījuma ceļa, proti, no lietotāja līdz rekursīvajam DNS serverim. Tālākais ceļš no rekursīvā DNS servera līdz pārējiem NS serveriem, ieskaitot saknes jeb root serveri, netiek šifrēts. Šeit ir darbs industrijai kopumā pie dažādu risinājumu ieviešanas, lai arī tālākais DNS plūsmas ceļš būtu šifrēts un nodrošinātu mūsu datu konfidencialitāti.



Ilustrācija 1: DNS šifrēšana ar DoT un DoH

Ir ieviests risinājums iepriekš aprakstītajai problēmai - protokols, kuru dēvē par **DNS vaicājuma minimizēšana** (*DNS Query Name Minimization*), kas darbojas sekojoši - ja vēlaties apmeklēt vietni blog.piemers.lv, saruna starp rekursīvo DNS serveri un pārējiem NS izskatīsies šādi:

> Interneta saknes serverim tiek prasīts:
> "Vai jūs pazīstat . lv NS?"
> Atbilde:
> "Jā, te ir viņu IP adrese"
> Pēc tam .lv NS tiek jautāts:
> "Vai jūs zināt, kur atrodas piemers.lv?"
> Atbilde:
> "Jā, protams, lūdzu Jums piemers.lv NS IP adrese"
> Visbeidzot, piemers.lv NS tiek prasīts:
> "Kur atrodas blog.piemers.lv? "
> Atbilde:
> "Tas atrodas šeit - 123.123.123.123"

Tādā veidā vienīgais serveris, kas uzzina pilnu pieprasītā resursa nosaukumu, ir piemers.lv NS serveris, un tas ir arī vienīgais serveris, kuram tas būtu jāzina. Visiem pārējiem serveriem tiek nosūtīta tikai daļa no vaicājuma. Tas gan nepalīdz lietotājam palikt pilnīgi anonīmam, tomēr samazina sniegto datu apjomu.

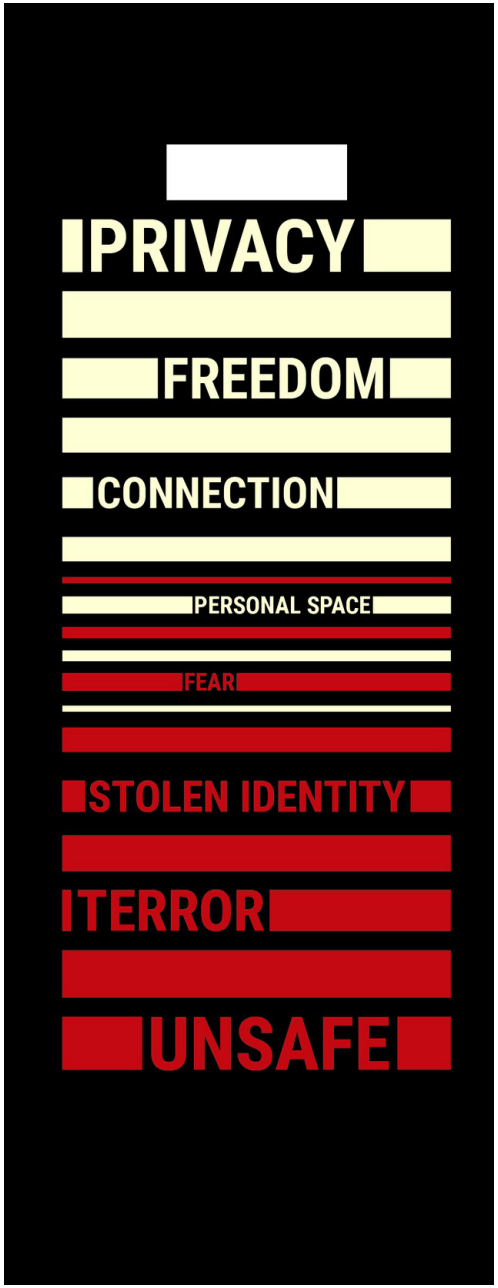
Taču jāapzinās, ka, apmeklējot kādu tīmekļa vietni, var nostrādāt arī daudzi citi faktori un savienojumi, kuri diemžēl joprojām notiek atklātā tekstā un tādēļ var "nopludināt" informāciju, kuru vēlējāmies aizsargāt, izvēloties DNS datu plūsmas šifrēšanu. Piemēram, *TLS server name indication*, drošības sertifikāta statusa pārbaude, *TLS resumption* un citi. Tādēļ IT nozarei kopumā ir vēl daudz jāstrādā pie citu protokolu un programmatūru pilnveidošanas.

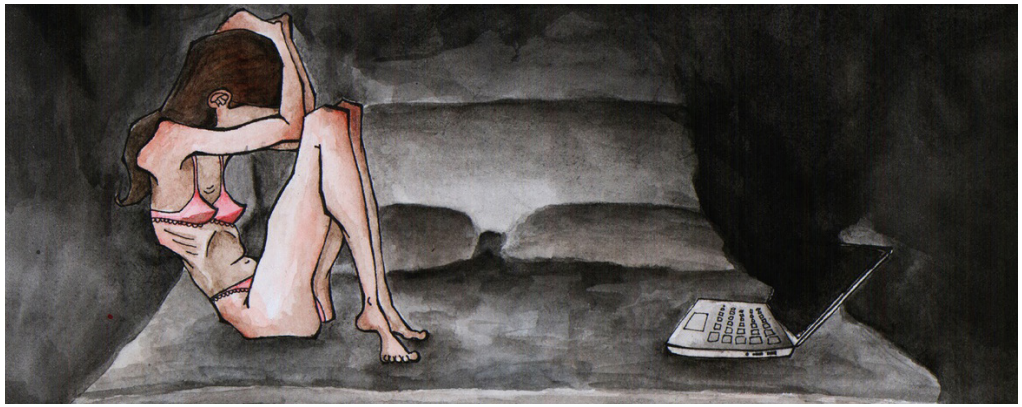
NIC REKURSĪVAIS DNS SERVERIS – CACHE.NIC.LV

NIC DNS rekursīvajam serverim ir cienījama 25 gadu gara vēsture. Tas tika izveidots jau tālajos "iezvana laikos", kad interneta pieslēgumi bija ļoti lēni. Neskatoties uz to, LU Matemātikas un informātikas institūtam bija pieejami labi starptautiski pieslēgumi, un, interneta infrastruktūras veiktspējas uzlabošanas nolūkos, tika nolemts izveidot DNS rekursīvo serveri.

> **CACHE.NIC.LV**
>
> **IPv4 adrese: 91.198.156.20**
> **IPv6 adrese: 2001:678:84::0**

Jau no sākta gala NIC nodrošina šo pakalpojumu Latvijas sabiedrībai bez maksas. Šo 25 gadu laikā neesam glabājuši žurnālfailus un tos monetizējuši, kā arī neplānojam to darīt.





Laikam ejot, esam savu DNS serveri ievērojami uzlabojuši:

- **Iespējota DNSSEC validācija** — DNSSEC ļauj pārliecināties, ka DNS atbildes saturs nav mainīts - nodrošina DNS datu autentifikāciju (plašāk par DNSSEC lasiet mūsu Reģistratūras avīzes #2). DNS serveris var veikt DNSSEC validāciju un automātiski bloķēt mājaslapas ar nekorektiem DNSSEC parakstiem, tā aizsargājot lietotāju no "*man in the middle*" uzbrukumiem.

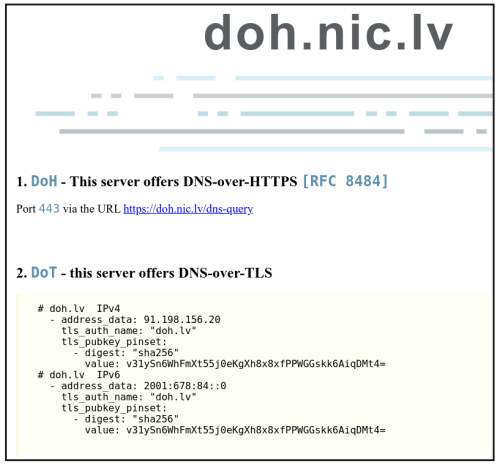
> ***"Man in the middle"* uzbrukums – DNS atbildes viltošana. Lietotāja pieprasījumu atvērt tīmekļa vietni pārtver ļaundaris, kurš leģitīmās vietnes vietā lietotāju novirza pavisam uz citu lapu. Vizuāli jaunās lapas adrese ir tieši tāda, kādu pieprasījis lietotājs. Arī saturiski lapa var būt ļoti vai pat pilnīgi līdzīga. Rezultātā uzbrukuma upuris, to pat nenojaušot, var sniegt uzbrucējam savus datus. Sekas tam var būt visdažādākās!**

> Jautāsiet, vai DNS šifrēšana aizvieto DNSSEC? Atbilde ir nē! DoH un DoT nodrošina konfidencialitāti, savukārt DNS drošības paplašinājums DNSSEC - datu integritāti. DNSSEC nav veidots, lai aizsargātu no tīkla saziņas noklausīšanās vai vērošanas. Visiem šiem drošības protokoliem - DoH vai DoT un DNSSEC ir jāstrādā kopā!

- **CERT.LV DNS ugunsmūris (DNS RPZ*)** — ugunsmūra mērķis ir pasargāt tā lietotājus no apdraudējumiem, kas nāk gan no Latvijas, gan ārpus tās. Apdraudējumu datu bāzi uztur un regulāri atjauno CERT.LV.

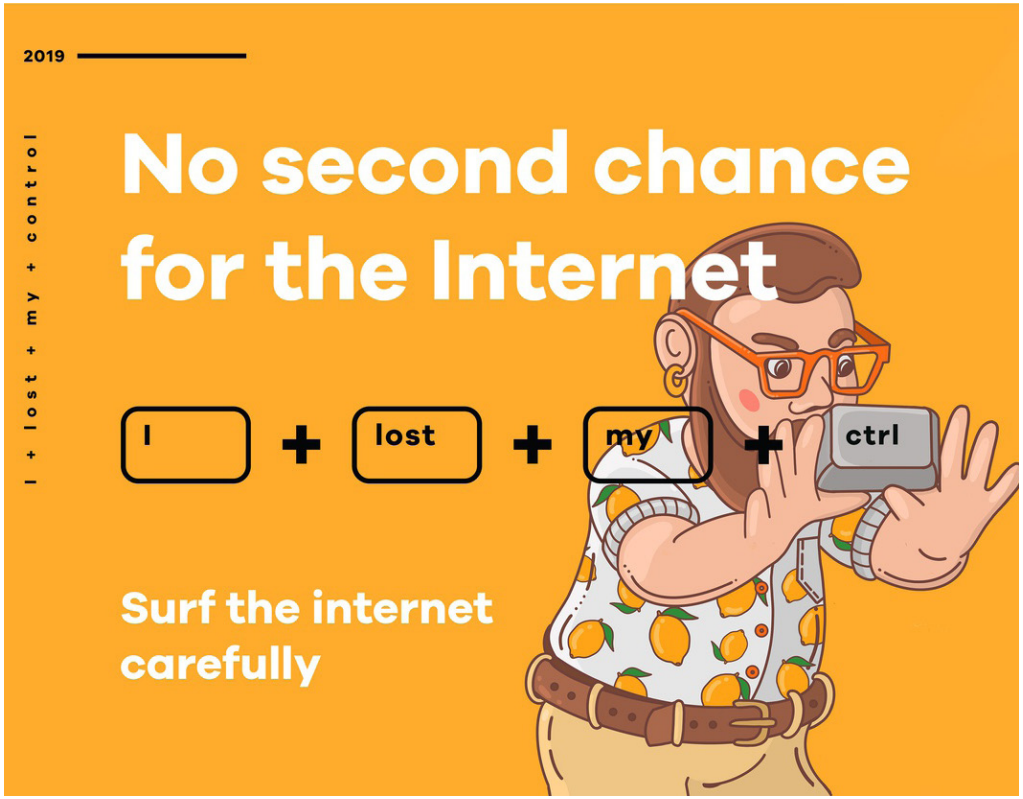
> Tā efektivitāti pastiprina arī fakts, ka CERT.LV ir pieejama arī reģionāla rakstura uzbrukumu analīze, tādēļ šis ir vienīgais DNS ugunsmūris, kas var izķert arī lokāla mēroga mērķētus uzbrukumus.

Sistēma nodrošina aktīvu aizsardzību, tā novēršot piekļūšanu bīstamajiem resursiem un pārvirzot tos uz brīdinājuma vietnes mērķlapu (*landingpage*). Arī gadījumos, kad ļaunatūra jau ir inficējusi kādu iekārtu, DNS ugunsmūris sniedz iespēju ātrāk identificēt šādas iekārtas, kas sistēmu administratoriem dod iespēju operatīvi veikt seku novēršanu.



Domēna vārdu sistēmas reaģēšanas politikas zona (DNS RPZ) ir metode, kas ļauj DNS servera administratoram pielāgot globālo DNS informāciju, lai nodrošinātu modificētas atbildes uz jautājumiem. Plašāk par DNS RPZ lasiet Reģistratūru avīze #4.

> Secinājums ir viens: interneta lietotāji novērtē savu datu privātumu un arvien biežāk izvēlas DNS šifrēšanu. Taču mums būtu jāmēģina izvairīties no datu plūsmas nokļūšanas viena IPS rokās. Tādēļ mēs, NIC aicinām ikvienu IPS rīkoties atbildīgi un iespējot DNS plūsmas šifrēšanu savos DNS serveros, tā radot lielākas izvēles iespējas mūsdienu digitālā privātuma nomāktiem interneta lietotājiem.



SPILGTĀKĀ .LV REĢISTRATŪRA!

Profesionāla pieeja un individuāla attieksme katram klientam – tāda ir 2019.gada nogalē NIC izvēlētās spilgtākās .LV Reģistratūras - RegiSTAR misija.

REGISTAR – SIA DATATEKS JEB SERVERIS.LV

Kā jau ierasts katrā .LV Reģistratūru avīzes numurā iepazīstinām lasītājus ar kādu no .LV Reģistratūrām. Šoreiz vēlamies izcelt vienu no ilggadīgiem NIC klientiem - SIA Datateks, plašāk pazīstamu mūsu klientiem kā serveris.lv. Lai gan par pilntiesīgu .LV Reģistratūru uzņēmums kļuva tikai 2019. gadā, visu serveris.lv pastāvēšanas laiku tā pārraudzībā ir bijis ievērojams skaits .LV domēna vārdu, par kuriem tas allaž ir rūpējies ļoti vērīgi, ievērojot savu gala klientu vēlmes, intereses, nepieviļot to uzticību.

Dažos vārdos raksturojot NIC sadarbību ar serveris.lv, gribētos teikt: kvalitāte, pieredze, lojalitāte un operatīva rīcība.

SIA Datateks, izmantojot zīmolu serveris.lv, saviem klientiem nodrošina plašu pakalpojumu klāstu: domēnu vārdu reģistrāciju ne tikai .LV, bet arī daudzos citos augstākā līmeņa domēnos, Linux un Windows hostinga un virtuālo serveru pakalpojumus, serveru nomu un daudzus citus ar mājas lapu izveidošanu, uzturēšanu un administrēšanu saistītus pakalpojumus. Īpaša uzmanība tiek pievērsta drošībai, pastāvīgam monitoringam un rezerves kopiju veikšanai visiem klientiem, uzsverot, ka tehnisko atbalstu sniedz tāpat kā NIC 24 x 7. Serveris.lv apkalpo un savus pakalpojumus piedāvā gan privātpersonām, gan maziem, vidējiem un lieliem uzņēmumiem.

Serveris.lv ir viens no vadošajiem mājas lapu un e-pastu uzturēšanas (hostings) pakalpojumu sniedzējiem Latvijā. Serveris.lv izveidots 2002.gadā un, pateicoties profesionāliem pakalpojumiem un tehniskā atbalsta nodrošināšanai, kas optimāli samērota ar cenu līmeni, iegūta augsta klientu uzticība.

"Jebkuru no mūsu pakalpojumiem iespējams atbilstoši pielāgot klientu tehniskajām vajadzībām un finansiālajām iespējām. Ikviens klients pie mums ir īpašs!"

SIA DATATEKS

VĒRTĒŠANAS KRITĒRIJI	VĒRTĒJUMS
NIC pakalpojumu pielietojums (tradicionālie un latviskie domēna vārdi, NICEPP, DNSSEC)	★★★
Domēna vārdu portfeļa izaugsme	★★★★★
Reģistratūras klientu atsauksmes	★★★★★
Laicīga maksājumu veikšana	★★★★★
Sadarbība ar NIC (DNS administratori, tehniskie risinājumi, PR)	★★★★
Dalība NIC pasākumos	nav
Dalība NIC projektos	nav

KĻŪSTI PAR .LV REĢISTRATŪRU UN SAŅEM PRIEKŠROCĪBAS:

35% Atlaide domēna vārdiem, ja domēna vārdu skaits > 50

50% Atlaide visiem DNSSEC parakstītiem domēna vārdiem

Ātrāka & ērtāka domēna vārdu reģistrēšanas procedūra. Reģistrētais domēna vārds sāk darboties **30 min** laikā.

PLAŠĀKAS PILNVARAS:

- Labo esošā domēna vārda lietotāja kontaktinformāciju.
- Izveido jaunu domēna vārda lietotāju vai izvēlies lietotāju no savu klientu saraksta.
- Maini administratīvo un tehnisko kontaktpersonu.
- Labo un pievieno jaunu domēna vārda tehnisko informāciju.
- Saņem rēķinu tikai reizi mēnesī.
- Atsakies no apmaksas par domēna vārdiem, kuri ir iekļauti tekošajā rēķinā.
- Veic domēna vārdu Reģistratūras maiņu.
- Atsakies turpmāk pārvaldīt domēna vārdu.

DNSSEC

Piedāvā .lv domēna vārdu reģistrēšanu un to parakstīšanu ar domēna vārdu sistēmas drošības paplašinājumu

Jaunām reģistratūrām kā atspēriena platformu piedāvājam reģistrēt un pārvaldīt domēna vārdus, izmantojot NIC klientu tiešsaistes sistēmas reģistratūras profilu

24/7 ATBALSTS

Tel: +371 67085858
e-pasts: registrars@nic.lv
+
informatīvi materiāli un izglītojoši pasākumi par domēnu industriju

DOMĒNA VĀRDU PĀRVALDĪŠANAS RISINĀJUMS NICEPP

- Pārvaldi un reģistrē domēna vārdus 24/7.
- Automatizē domēna vārda pārvaldību, saskaņojot savu datu bāzi ar .lv reģistrā esošo informāciju.
- Pielāgo izveidoto risinājumu sadarbībai ar citu domēnu reģistru uzturētājiem.
- Izveido tīmekļa saskarni saviem klientiem.

SKAITĻI UN FAKTI 2019

125 640

Kopējais reģistrēto .LV domēna vārdu skaits

(07.02.2020.)

Aktīvākais d/v reģistrācijas mēnesis:

jūlijs

kurā reģistrēti:

3628

jauni domēna vārdi

Populārākais raksts:

Atsakies no domēna vārda atbildīgi

(2200 statījumu)

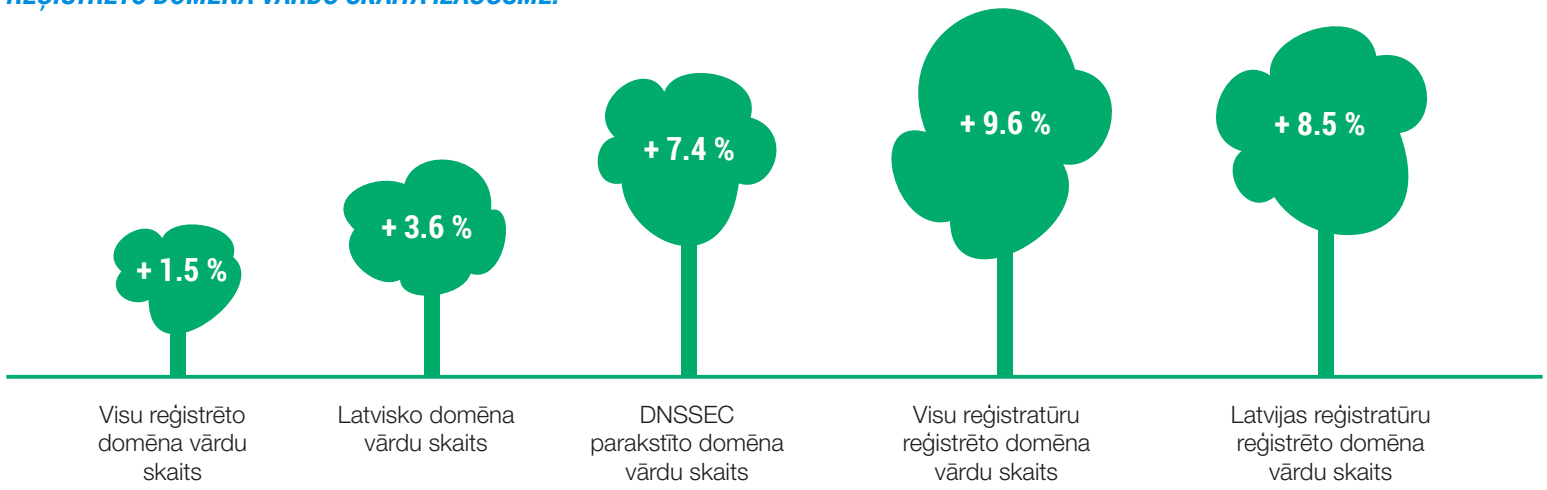
NIC pārstāvji šajā periodā uzstājušies

8 semināros,

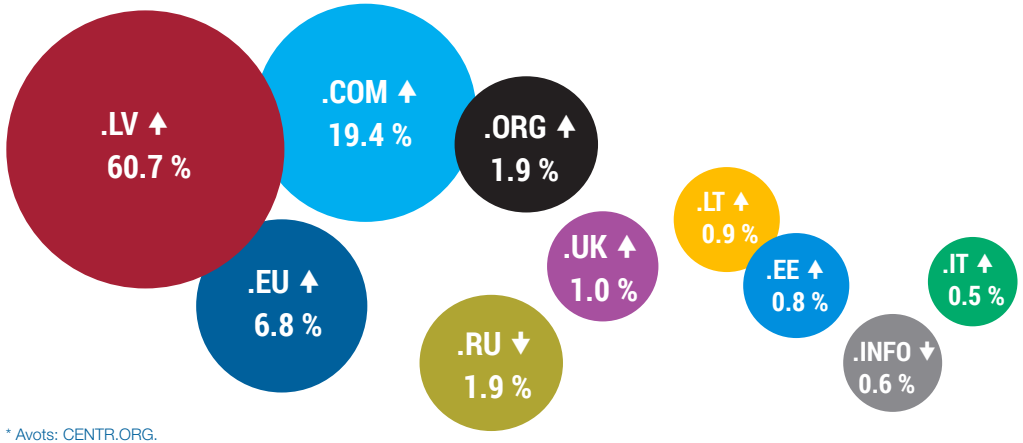
izglītojot

1832 dalībniekus

REĢISTRĒTO DOMĒNA VĀRDU SKAITA IZAUGSME:



LATVIJAS UZŅĒMĒJU UN IEDZĪVOTĀJU IECIENĪTĀKIE DOMĒNI:



* Avots: CENTR.ORG.

LATVIJAS INTERNETA LIETOTĀJU APMEKLĒTĀKĀS VIETNES:

1. google.com
2. youtube.com
3. inbox.com
4. google.lv
5. ss.com
6. vk.com
7. e-klase.lv
8. delfi.lv
9. swedbank.lv
10. aliexpress.com

* Avots: Alexa statistika, 2019. oktobris.