.LV

REĢISTRATŪRU AVĪZE

2019
#8
www.nic.lv

ŠAJĀ NUMURĀ LASIET:

DROŠA DOMĀŠANA!

Atceroties mūsu pēdējo .LV Reģistratūru konferenci Rīgas Motormuzejā, nodomāju, cik gan lielas pārmaiņas ir piedzīvojušas auto un IT industrijas, kas dekādes laikā ir attīstījušās ar eksponenciālu ātruma pieaugumu.

Nav izslēgts, ka pavisam drīz jau ierasta lieta būs uz ielām redzēt pašbraucošas automašīnas, taču visdrīzāk to vadības bloki joprojām izmantos DNS pieprasījumus, piemēram, lai atrastu attālinātu sistēmu, kurai ziņotu par auto pārvietošanās ātrumu, stūres leņķi un citiem parametriem. Šādas sistēmas prasīs vēl lielāku iedziļināšanos drošības jautājumos, tajā skaitā, tādos, kas saistīti ar drošu komunikācijas protokolu izmantošanu.

> Ne velti, jau 2013. gadā NIC veica .LV zonas parakstīšanu ar DNSSEC, tomēr reģistratūru un lietotāju interese par DNSSEC ir vērtējama kā zema, jo pašlaik tiek parakstīti vien 3,2% .LV domēna vārdu. Jāpatur prātā, ka šobrīd uz DNS infrastruktūras balstās arī citi ar drošību saistīti protokoli, kā, piemēram, DMARC, DKIM, SPF, DANE u.c, kuru ieviešanā daudzas Eiropas valstis Latviju ir krietni apsteigušas.

Ir sagaidāms, ka klienti, kuri izmanto reģistra un reģistratūru sniegtos pakalpojumus, nākotnē arvien biežāk pievērsīs uzmanību drošības aspektiem. Tādēļ drošības paplašinājumu pieejamība būs piedāvātā pakalpojuma obligāta un pašsaprotama sastāvdaļa!

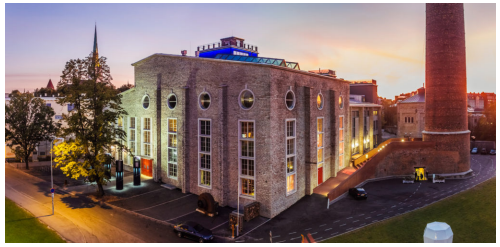
Būtu lieliski, ja mēs kopīgiem spēkiem varētu salikt šo drošības mozaīku, ieviešot vismaz kādu no drošības uzlabojumiem, tā padarot mūsu sistēmas mazāk pievilcīgas uzbrucējam.

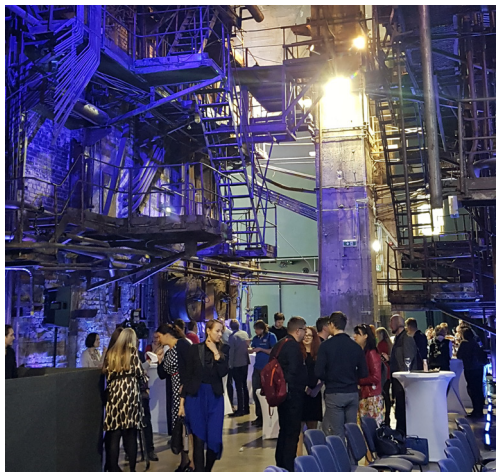
NIC aicina apmeklēt 11.-12. septembrī TLD-CON 2019 un 2.-3. oktobrī CERT.LV organizēto ikgadējo IT drošības konferenci “Kiberšahs 2019”, kuras varēs vērot arī tiešsaistē, kā arī CENTR organizētos pasākumus, vairāk par pasākumiem 7.lpp.

Domājam droši!

Ar cieņu,
Ivo Ķutts
.LV reģistra (NIC) tehniskās nodaļas vadītājs

Paldies visiem, kuri ieradās Tallinā uz ikgadējo Baltic Domain Days 2019 konferenci, kā arī apmeklēja tepat Rīgā rīkoto semināru “Internet Identifier Threats and Security Challenges”!





ATSAKIES NO DOMĒNA VĀRDA ATBILDĪGI

Neatkarīgi no tā, vai esat nolēmis mainīt vai izbeigt zīmola, projekta, reklāmas kampaņas vai tīmekļa vietnes darbību, pārdot vai apvienot uzņēmumu, var šķist nekaitīgi un loģiski arī atteikties no sava "vecā" domēna vārda. Taču ne velti bankas no reiz lietotiem domēna vārdiem neatsakās! Piemēram, "Swedbank" ir mainījusi nosaukumu no "Hansabanka" 2009. gadā, bet plaši izmantoto domēna vārdu hanzanet.lv ir saglabājis.

Kad domēna vārda lietošanas termiņš beidzas un tā lietotājs nolemj to nepagarināt, domēna vārds pēc 30 dienu pārejas perioda kļūst publiski pieejams reģistrācijai jebkuram interesentam.

Atteikšanās no reiz lietota domēna vārda var radīt drošības riskus ne tikai pašam uzņēmumam, tā zīmolam un darbiniekiem, bet arī klientiem un sadarbības partneriem!

Pirms pieņemt lēmumu - atteikties no domēna vārda, iesakām iepazīties, izvērtēt un nodrošināties pret iespējamiem riskiem, kas bieži vien domēna vārda lietotājam paliek nepamanīti.

Atšķirībā no "drop catchers" un domēna vārdu skvoteriem (kas reģistrē domēna vārdu pēc tam, kad tas nav pagarināts un mēģina to pārdot iepriekšējam lietotājam vai konkurentam jau par lielāku cenu), hakeriem ir vairāki veidi, kā izmantot reiz lietotu domēna vārdu.

2018. gada vidū informācijas tehnoloģiju drošības uzņēmuma "Possible Security" vadošais pētnieks K.Solovjovs ar savu komandu veica pētījumu – piereģistrēja 180 tikko atbrīvojušos .LV domēna vārdus un veica kvantitīvu un kvalitatīvu saņemto datu analīzi, t.sk. saglabājot FTP, SSH, TELNET, SMTP, DNS, HTTP, POP3, IMAP, HTTPS, RDP, VNC protokolos saņemtos pieprasījumus.

Ar "Possible Security" pētījuma gaitu un rezultātiem var iepazīties YouTube.

Analizējot pētījuma rezultātus, var secināt, ka vecs un nevajadzīgs, reiz lietotais domēna vārds, šķiet tikai tā iepriekšējam lietotājam, bet ne internetam kopumā.

Tīmekļa pieprasījumu un saņemto e-pastu skaits un saturs liecina, ka domēna vārds pat pēc tā "nāves" ir pieprasīts un ļaundara rokās var kalpot, kā "zelta atslēga uz visiem uzņēmuma kiberdrošības cietokšņiem."

AR KO UZŅĒMUMS RISKĒ?

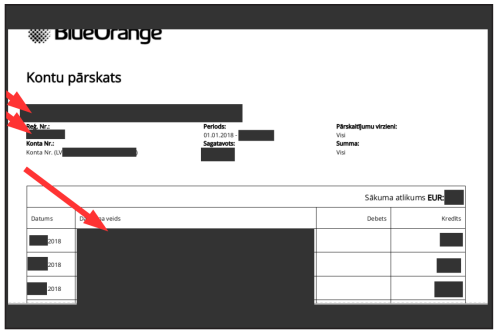
Domēna vārds ir kā vārti uz citiem tiešsaistes pakalpojumiem, kas padara to par lielisku mērķi kiberuzbrukumiem!

Piereģistrējot Jūsu veco domēna vārdu, jaunais lietotājs var iegūt kontroli pār tā saturu, vecajām e-pasta adresēm un web pieprasījumiem, līdz ar to rodas iespējas kriminālām darbībām.

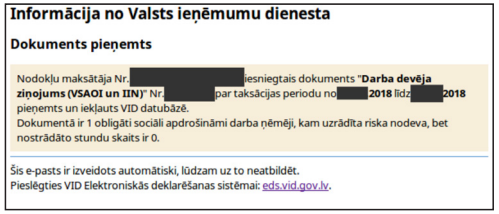
1. SAŅEMT KONFIDENCIĀLU VAI PRIVĀTU INFORMĀCIJU

Lai cik publiski aktīvi uzņēmums sludinātu par sava jaunā zīmola un domēna vārda maiņu, klienti, ieraduma vai vienkārši e-pasta programmas iestatījumu dēļ, sazināsies ar Jums izmantojot sev ierasto (Jūsu acīs veco) domēna vārdam piesaistīto e-pasta adresi. Tādēļ liela daļa klientu var turpināt pēc domēna vārda dzēšana pārsūtīt savu konfidenciālo informāciju jaunajam domēna vārda lietotājam. Bieži tiek piemirsti arī sadarbības partneri (tādi kā bankas un ar Jūsu darbību saistītās valsts vai pašvaldību iestādes), kuras savukārt būtu atsevišķi jāinformē par sava kontakta e-pasta adreses maiņu.

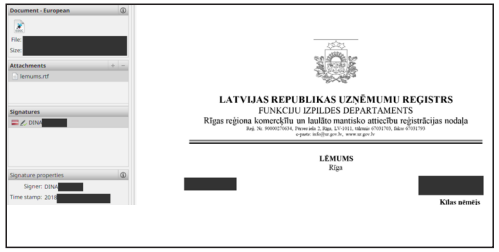
K. Solovjova pētījumā tika novērots, ka 30% no e-pastiem, kas tika sūtīti uz tikko reģistrētajiem domēna vārdiem, saturēja kādus pielikumus, no kuriem 22% bija .pdf vai .doc formātā, šāda veida pielikumi var saturēt uzņēmuma vai to darbinieku konfidenciālu informāciju. Lūk dažas no pētījuma laikā saņemtajām vēstulēm (visa personīgā informācija ir aizklāta):



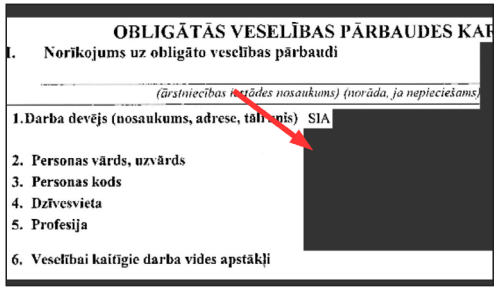
Informācija no bankas, uzņēmuma konta pārskats (satur konfidenciālu finanšu informāciju).



Informācija no valsts iestādēm, kā, piemēram, VID.

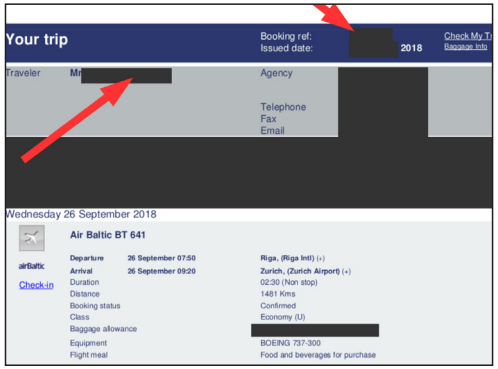


Elektroniski parakstīti dokumenti.

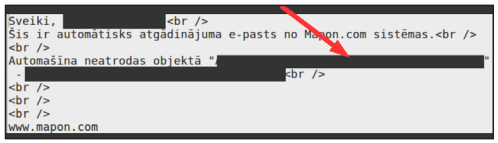


Sensitīva informācija no medicīnas iestādēm.

Pētījumā tika atklāts, ka šajā konkrētajā gadījumā tika izmantota šifrēšana un parole, taču parole nebija pietiekami droša. Laba šifrēšana ir papildus drošības līmenis!



Aktuāli uzņēmuma pasūtījumi, rezervācijas apstiprinājumi, kuri var saturēt Jūsu un Jūsu darbinieku vai sadarbības partneru konfidenciālu informāciju, atsevišķos gadījumos, kad pasūtījums ir apmaksāts, uzbrucējs var viegli iegūt labumu sev.



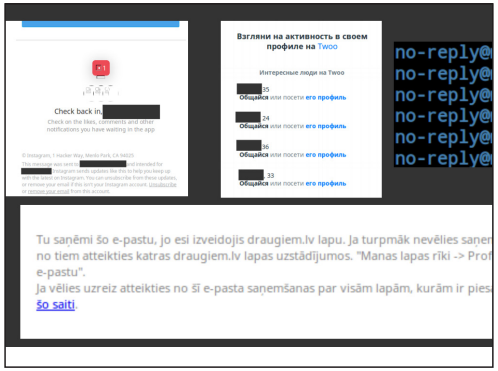
Automātiski izsūtītā informācija no GPS izsekošanas ierīcēm.

Informācija no sadarbības partneriem, konkrētajā gadījumā no zvērināta advokāta (var saturēt arī komercnoslēpumu).

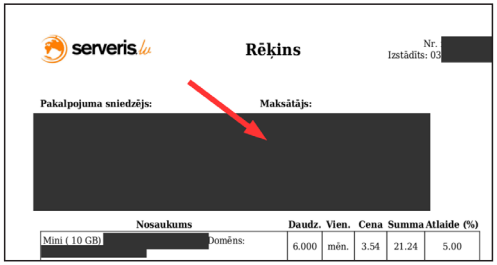
2. IEGŪT PIEEJU JŪSU UN JŪSU DARBINIEKU TIEŠSAISTES PAKALPOJUMU KONTIEM

Nav noslēpums, ka darbinieki mēdz norādīt darba e-pasta adresi, kā kontakta adresi vai lietotājvārdu arī saviem personīgajiem tiešsaistes pakalpojumu kontiem (kā, piemēram: Facebook, draugiem.lv, vid.gov.lv, utt.). Jaunais domēna vārda lietotājs, izveidojot identisku e-pasta adresi un izmantojot paroles atjaunošanas funkciju, var iegūt kontroli pār šiem kontiem. Savukārt, ja kāds no šiem sociālo tīklu profiliem ir piesaistīts arī uzņēmuma profilam, uzbrucējs var izplatīt dezinformāciju ar mērķi bojāt uzņēmuma reputāciju.

Lūk, daži praktiski piemēri no pētījuma:



Paziņojumi no uzņēmuma vai to darbinieku sociālajiem tīkliem.



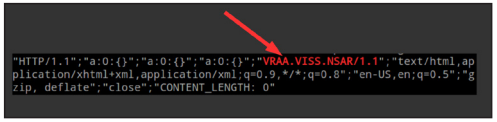
Rēķini un atgādinājumi. Daži pakalpojumu sniedzēji ļauj identificēties izmantojot klienta vai rēķina numuru, iegūstot šo informāciju, uzbrucējs var pieslēgt vai atslēgt sev vēlamos pakalpojumus.

3. PĀRVALDĪT VAI DEZINFORMĒT JŪSU TĪMEKĻA VIETNEI PIESAISTĪTĀS SISTĒMAS

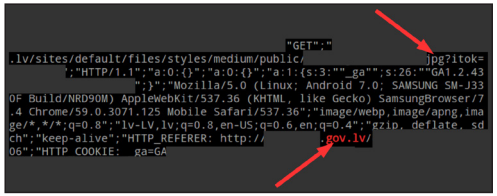
Informāciju, ko jaunais domēna vārda lietotājs saņem e-pastā, var izmantot jebkurš pat bez īpašām IT zināšanām. Tomēr tas nav viss arsenāls, ko var saņemt jūsu vecā domēna vārda jaunais lietotājs. Piereģistrējot kāda uzņēmuma lietotu domēna vārdu, uzbrucējs var iegūt arī kontroli pār ienākošajiem tīmekļa pieprasījumiem no citām vietnēm un sistēmām, kas var saturēt nepieciešamo informāciju, lai iegūtu kontroli pār uzņēmuma serveriem.

Lūk, daži no pētījuma laikā saņemtajiem tīmekļa pieprasījumiem:

Ieplānoti pieprasījumi no pamesta Wordpress. Uzbrucējs var noskaidrot, kāda WordPress versija tiek izmantota, un izmantojot tā trūkumus iekļūt vecajā serverī.



Valsts informācijas sistēmas savienotāja pieprasījumi, kas konkrētajā gadījumā rada risku, ka uzbrucējs varētu censties izveidot neautorizētu savienojumu ar Valsts informācijas sistēmām.



Latvijas valsts (gov.lv) vietnes iegulti html elementi. Tādējādi var daļēji kontrolēt sadarbības partneru, šajā gadījumā valsts iestāžu, mājaslapu saturu.

4. BOJĀT ZĪMOLA REPUTĀCIJU

Visbiežāk reiz lietotus domēna vārdus reģistrē uzņēmumi, kuri vēlas uzlabot savas jaunās tīmekļa vietnes apmeklējumu statistiku, izmantojot Jūsu vecā domēna vārda vēl esošo tīmekļa plūsmu un backlinkus (norādes uz tīmekļa vietni no citām vietnēm). Īpaši vērtīgi ir valsts iestāžu, kā arī tiešo konkurentu vecie domēna vārdi, jo pastāv iespēja veikli pārvilināt konkurenta klientus pie sevis. Šāda veida populāru vai Jums vēlamo apmeklētāju iecienītu zīmolu izmantošana sava labuma gūšanai ir ļoti izplatīta visā pasaulē. Ja tīmekļa vietne, uz kuru tiek pārsūtīti jūsu uzticamie klienti, ir neglaimojoša satura, tad tas var bojāt arī Jūsu zīmola reputāciju.

SECINĀJUMI: KĀ SEVI AIZSARGĀT?

Viss atkarīgs kāda veida uzņēmums, iestāde vai organizācija esat. Bieži vien labāk būt drošam nekā nožēlot! Domēna vārdi nav dārgi.

> **Reiz lietota domēna vārda glabāšana var izrādīties lētākā kiberdrošības adprošināšanas polise pasaulē!**

DOMĒNA VĀRDA MAIŅAS GADĪJUMĀ, NEPIECIEŠAMS IZVĒRTĒT SEKOJOŠAS IESPĒJAS

- Laicīgi un uzstājīgi informēt ne tikai savus klientus, bet arī sadarbības partnerus, kā arī trešās personas, kas izmanto jūsu domēna vārdu vai tam piesaistītu API, par domēna vārda un attiecīgi arī Jūsu kontakta e-pasta adrešu maiņu;
- Paturēt[1] lietoto domēna vārdu vismaz nākamos pāris gadus, lai:
  - neļautu surogātpasta sūtītājiem (vai konkurentiem) to pārņemt. Tādā veidā arī nodrošinoties, ka neviens cits nevar izlikties par Jūsu uzņēmumu vai zīmolu tiešsaistē, saglabājot uzņēmuma labo vārdu un neļaujot citiem izmantot Jūsu zīmola reputāciju;
  - pārsūtīt visu tīmekļa datu plūsmu un e-pastus uz jaunajam domēna vārdam piesaistītajiem e-pastiem un tīmekļa vietni.[2] Tādā veidā uzskatāmi informējot par izmaiņām e-pastu sūtītājus un vecās tīmekļa vietnes apmeklētājus, dodot laiku jūsu klientiem un sadarbības partneriem pierast pie izmaiņām;
- Pārdot vai nodot savu domēna vārdu lietošanā citam interesentam, par kura reputāciju esat pārliecināts, un zināt, kādam mērķim domēna vārds tiks izmantots;
- Atsaistīt vecās e-pasta adreses no visiem tiešsaistes pakalpojumu kontiem, kā arī aicināt savus darbiniekus rīkoties līdzīgi, izglītot par sekām, kādas var rasties, ja tas netiks darīts;
- Izmantot un ieviest kiberdrošības pamatnoteikumu - drošas paroles un divu faktoru autentifikāciju.

Ja iestādes vai organizācijas darbība tiek izbeigta pavisam, izmantojiet savu veco domēna vārdu un tīmekļa vietni, lai informētu tās apmeklētājus par uzņēmuma darbības beigšanu. Laba prakse ir sniegt nepieciešamo informāciju arī saviem bijušajiem klientiem par to, kā rīkoties problēmu gadījumā.

1. Ja plānojat uzņēmuma darbību beigt, taču esat nolēmis paturēt tā domēna vārdu, nepieciešams laicīgi veikt domēna vārda lietošanas tiesību turētāja maiņu.

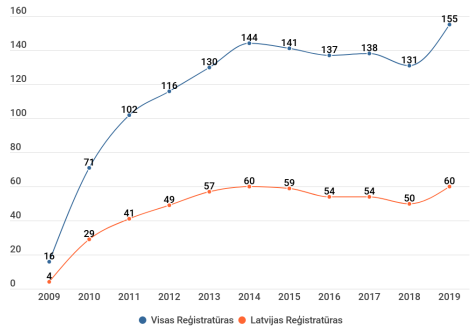
2. Šajā laikā savās iecienītākajās statistikas vai analītikas programmās pavērojiet, cik liela tīmekļa datu plūsma tiks zaudēta, ja pāriesiet tikai uz jauno domēna vārdu. Ja secināt, ka pietiekoši liels apmeklētāju skaits ir iecienījuši arī jūsu veco domēna vārdu, saglabājiet to, savukārt, ja redzat, ka tas netiek aktīvi lietots, varat atteikties no tā jau laicīgāk.

.LV REĢISTRATŪRU TIKŠANĀS 2019

23. maijā Rīgas Motormuzejā tika aizvadīta NIC ikgadējā ".LV Reģistratūru konference", kurā tika runāts par pasaules un Latvijas domēnu industrijas aktualitātēm un izaicinājumiem, valsts pieņemto lēmumu ietekmi uz .lv domēna attīstību, .lv domēna drošību, .LV Reģistratūru raksturiezīmēm, kā arī riskiem, kuri rodas, ja domēna vārda lietošanas tiesības nolemts nepagarināt. Šogad tikšanās bija īpaša - svinīgi atzīmējām mūsu sadarbības 'Reģistra – Reģistratūras' modeļa izveides desmitgadi.

2009. gada novembrī pēc .lv domēna vārdu reģistrācijas noteikumu liberalizācijas NIC ieviesa Reģistra – Reģistratūras modeli. Šis sadarbības modelis izveidoja uzņēmumiem, kuri sniedz vai vēlas sniegt .lv domēna vārda reģistrācijas pakalpojumus saviem klientiem, daudz ātrāku, ērtāku, kā arī finansiāli izdevīgāku vidi .lv domēna vārdu pārvaldīšanā, tajā pašā laikā aizsargājot .lv lietotāju intereses.

Tāpat kā .lv domēna vārdu un to lietotāju skaits, arī mūsu sadarbības partneru skaits šo 10 gadu laikā ir tikai audzis. Šobrīd .lv domēna vārdu piedāvā reģistrēt 157 oficiālās .LV Reģistratūras, no kurām diemžēl tikai 61 ir tepat no Latvijas.



.LV Reģistratūru skaita pieaugums

VISPLAŠĀKĀS DISKUSIJAS UN INTERESI KONFERENCĒ IZRAISĪJA

- pieaugošā lietotāju izvēle iegādāties .lv domēna vārdus izmantojot ārvalstu, nevis pašmāju reģistratūru sniegtos pakalpojumus. Šī tendence pēdējā laikā kļūst arvien izteiktāka, pagaidām reģistrēto domēna vārdu skaita ziņā "TOP 10" pirmās trīs vietas pieder Latvijas uzņēmumiem, taču, ja līdzīga tendence domēna vārdu tirgū turpināsies, tad situācija var arī mainīties, jo pārējās septiņas lielākās reģistratūras ir no ārvalstīm. Kāds ir pamats šādam pavērsienam, varam tikai minēt, bet noteikti tie nav finansiāli apsvērumi, jo dažas no lielākajām ārvalstu .lv reģistratūrām piedāvā .LV domēna vārdus pat par 50 EUR gadā.
- .lv domēna vārdu izaugsmes samazināšanās no ierastajiem 3% gadā uz 0,3% 2018. gadā. Šo samazināšanos var skaidrot gan ar likuma grozījumiem, kuri paredz tiesības VID, kā arī citām iestādēm pieprasīt .lv domēna vārda bloķēšanu, kā arī sarūkošo jauno uzņēmumu skaitu valstī kopumā.
- Vispārīgās datu aizsardzības regulas (turpmāk regula) ietekme uz reģistratūru darbību un skaitu. Stājoties spēkā regulai, NIC veica vairākus grozījumus, tajā skaitā arī Reģistra-Reģistratūru līgumā, ieviešot jaunu pielikumu par personas datu apstrādi. Daļa reģistratūru šo pielikumu nevēlējās parakstīt, tādēļ līgumi ar šīm iestādēm tika lauzti. Semināra laikā NIC un reģistratūras dalījās pieredzē ar saviem rīcības plāniem personas datu noplūdes gadījumā.

.LV REĢISTRATŪRU KONFERENCE

23.05.2019, 10:00 – 13:30
RĪGAS MOTORMUZEJS, S.EIZENŠTEINA IELA 8, RĪGA

10.00 *Reģistrācija & saviesīgas sarunas pie siltas kafijas krūzes ar uzkodām*

10.30 Globālās un lokālās domēnu industrijas tendences.

K.Sataki (.LV reģistra vadītāja)

LV 25 vai tas ir daudz vai maz? Vērtēsim paveikto .lv domēna ieviešanā, attīstīšanā, sistēmu izstrādē, infrastruktūras izbūvē un tehnisko risinājumu modernizēšanā. Novērtēsim aizgājušo 2018. gadu - kāda ir bijusi .lv domēna, to lietotāju un reģistratūru attīstība un izaugsme? Kuri faktori šo izaugsmi ir stimulējuši, kuri - bremzējuši? Kas mūsu nacionālo digitālo identitāti sagaida nākotnē? Kādas ir pasaules domēnu industrijas tendences, aktualitātes un nākotnes vīzijas/projekti? Brexit & .EU - kas jāzina reģistratūrām, kas piedāvā .eu domēna vārdu reģistrāciju?

11.00 Kā valsts pieņemtie lēmumi ietekmē .LV domēna attīstību?

I.Skujiņa (.LV reģistra juriste)

Jau pagājis gandrīz gads, kopš ieviesta VDAR, kā tā ir ietekmējusi .lv domēna vārdu reģistrācijas kārtību un WHOIS pakalpojumu? Kas jāņem vērā Reģistratūrām? Kā atšķiras .LV, .LT un .EE pieeja VDAR ieviešanā?
Kādas vēl izmaiņas gaidāmas tuvākā nākotnē? Vai tās ietekmēs .lv reģistratūru darbību Latvijā? Cik aktīvi VID izmanto likumā piešķirtās tiesības atslēgt .lv domēna vārdus? NIS direktīva? Azartspēļu inspekcijas virzītie jaunie likuma grozījumi – kā tie mūs varētu ietekmēt?

11.30 Nu un kas, ja nepagarinu domēna vārdu?

K. Solovjovs (Possible Security vadošais pētnieks)

Domēna vārdi ir centrālais interneta "nekustamais īpašums" – gandrīz visa komunikācija ar organizāciju tiek veikta, izmantojot domēna vārdus (e-pasts, mājaslapa, TLS sertifikātu izrakstīšana). Tādēļ ir būtiski nepazaudēt kontroli pār domēna vārdu! Taču atšķirībā no būvēm, tos nav iespējams iegādāties, bet gan tikai īrēt – tas nozīmē ikgadējus tēriņus. Kādus labumus uzbrucējs var iegūt, pārņemot kontroli pār tikko "beigušos" domēna vārdu, kādus riskus tas rada domēna iepriekšējam lietotājam un kā pareizi sabalansēt šos riskus ar finansiālo ieguldījumu?

12.00 .LV prioritātes – drošība, privātums un stbilitāte.

I.Ķutts (.LV reģistra Tehniskais direktors)

Kas ir mainījies DNS dzīvē - DNSSEC saknes zonas atslēgas maiņa; DNS flag day; DNS RPZ;

12.20 ReReDra – Reģistrs Reģistratūrai Draugs.

D.Ludviga (.LV reģistra Mārketinga daļas vadītāja)

Atskatīsimies uz nozīmīgākajiem domēnu industrijas pasākumiem Latvijā, kuri aizvadīti 2018/2019 gadā - Baltic Domain Days 2018 & 2019, TLD-Con2018, CERT.LV & NIC sadarbība ar LTRK, RigaTechGirls, NIC skolās, CENTR Registrar Day un CENTR Admin Rīgā. "2019. gada domēnu industrijas pasākumu kalendārs".
Reģistratūru profils – uzzini, ko par tavu darbību liecina tava uzņēmuma statistika no pārvaldīto .lv domēna vārdu skatupunkta? Visiem klātesošiem dalībniekiem tiks izdalīta pārstāvošās Reģistratūras statistikas profils.*
Reģistra - Reģistratūras modelim jau 10 gadi. Kādas ir .LV Reģistratūras? Kuras no tām izvēlas lietotāji un kāpēc?

13.00 *Diskusijas neformālā gaisotnē pie 10 gadu jubilejas kūkas.*

13.30 Visiem dalībniekiem bezmaksas ekskursija gida pavadībā pa Rīgas Motormuzeju)

(Ekskursijas ilgums aptuveni 90 minūtes)

Pasākuma noslēgumā tika apskatīti gan nesen aizvadītie, gan tuvākā laikā plānotie domēnu industrijai veltītie semināri un konferences.

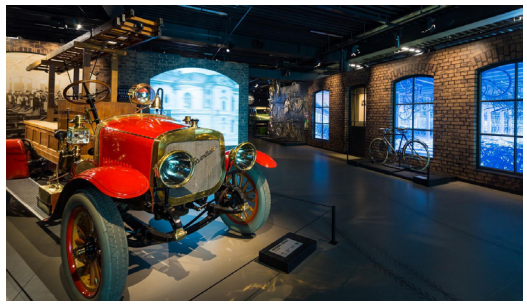
Atzīmējot mūsu sadarbības 10gadi, katram Reģistratūru pārstāvim bija iespēja aplūkot uzņēmuma pārvaldāmo .lv domēna vārdu statistikas apskatu jeb ielūkoties NIC topošajā statistikas portāla sadaļā "Reģistratūras profils", kas piedāvāja apskatīt un novērtēt ne tikai pārvaldāmo domēna vārdu, bet arī to lietotāju - Reģistratūru klientu skaita pieaugumu, kustību un tipu. Novērtēt, kuri ir aktīvākie un pasīvākie jaunu domēna vārdu reģistrēšanas mēneši, kā arī daudz ko citu. Drīzumā šis statistikas apskats būs pieejams arī visām pārējām Reģistratūrām.

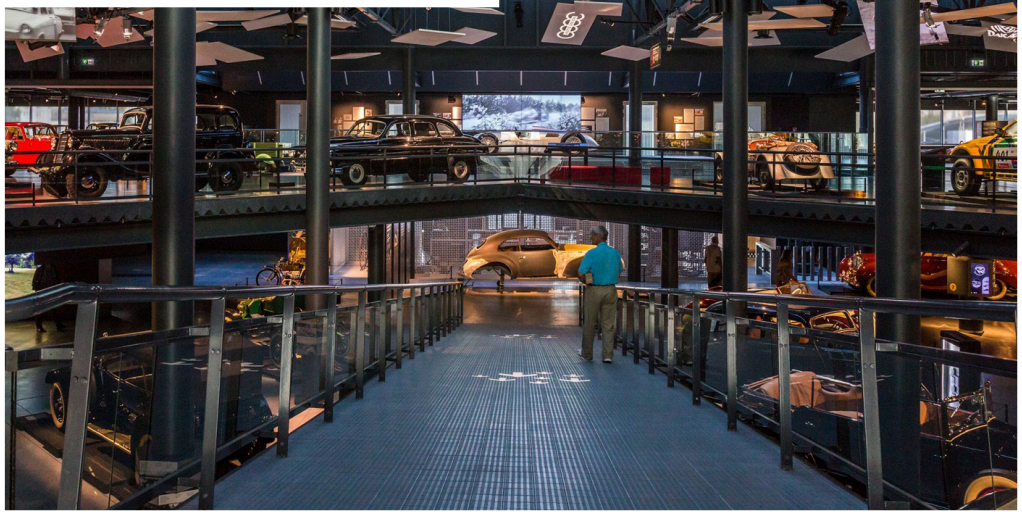
Par godu desmitgadei, pēc konferences tika organizēta ekskursija gida pavadībā, kuras laikā pasākuma apmeklētāji varēja iepazīt Rīgas Motormuzeja seno spēkratu stāstus, ekspozīciju un aktuālās izstādes.

Papildus tika pieaicināts vieslektors – "Possible Security" vadošais pētnieks, Kirils Solovjovs, kurš prezentēja sava praktiskā pētījumu rezultātus (reģistrējot ~150 tikko "beigušos" .lv domēna vārdu) par labumiem, kurus var iegūt uzbrucējs, pārņemot kontroli pār tikko "beigušos" domēna vārdu, kā arī riskiem, kuri rodas domēna vārda iepriekšējam lietotājam. Ar pētījuma rezultātiem tuvāk var iepazīties 2.lpp.

.LV Reģistratūru konferencē tika skaidrots, kādēļ vairāk šādas tikšanās ar vietējām reģistratūrām netiks rīkotas. 23. maijā tika aizvadīta pēdējā tikšanās tik tuvā reģistra un reģistratūru dalībnieku lokā. Tiksimies jau plašāku domēna industriju pasākumu ietvaros (Baltic Domain Days).

Aicinām visus sadarbības partnerus jautājumu vai neskaidrību gadījumā zvanīt vai nākt pie mums ciemos uz Raiņa bulvāri 29.





NIC AICINA APMEKLĒT

TLDCON 2019

.RU/.РФ reģistrs “Координационный центр доменов .RU/.РФ” aicina uz ikgadējo Centrālās un Austrumeiropas valsts koda domēnu reģistra uzturētājiem un reģistratūrām veltīto konferenci “TLDCON 2019”, kura norisināsies 11. - 12. Septembrī Viļņā (Lietuva), Grand Hotel Kempinski Vilnius. Dalība konferencē ir bezmaksas, iepriekšēja reģistrācija ir obligāta.

Atskats uz pagājušā gada konferenci TLDCON 2018, kura norisinājās tepat Latvijā, Jūrmalā, Baltic Beach Hotel viesnīcā ir pieejama:

- Angļu valodā
- Krievu valodā

Diskusiju paneļu un prezentāciju videoieraksti pieejami YouTube.

TLDCON

2019-09-11

9.30 **Registration and welcome coffee**
10.00 **Plenary meeting**
11.30 **Session 1. Cybersecurity: How registries collaborate with law enforcements**
14.30 **Session 2. Legal issues of domain name registration**
16.00 *Coffee*
16.30 **Session 3. Is there future for domain names?**
19.30 **Departure of buses to the gala dinner**

2019-09-12

9.30 **Registration**
10.00 **Session 4. Domain marketing: Face to face with end user**
11.30 *Coffee break*
12.00 **Session 5. Secondary market of domain registration**
13.30 *Lunch*

CENTR STARPTAUTISKĀ REĢISTRATŪRU DIENA

CENTR kopš 2014. gada savā darbībā iesaista arī Reģistratūras, ik gadu organizējot Starptautisko reģistratūru dienu (*CENTR Registrar Day*). Šī ir vieta un laiks, kad visi domēna industriju pārstāvji tiekas vienuviet – Eiropas augstākā līmeņa domēna turētāji satiekas ar reģistratūrām, kopīgi diskutējot un veidojot savstarpējus sadarbības projektus.

Nākamā Starptautiskā Reģistratūru Diena norisināsies 8. oktobrī Briselē, Beļģijā!

Ja vēlaties apmeklēt Starptautisko reģistratūru dienu, dodiet ziņu, rakstot uz pr@nic.lv palīdzēsim Jums reģistrēties un pieteikties.

Plašāka informācija par pasākumu pieejama šeit.

Council of European National Top-Level Domain Registries

REGISTRAR DAY AGENDA

2019-10-08

9.00 **Welcome and introduction**
9.10 **Registry-registrar speed-networking**
10.40 *Coffee break*
11.00 **Speed-networking (continued)**
11.10 **The role of eIDs in an age of data accuracy**
11.30 **Domain name market trends**

- Presentation of most recent market trends
- Panel discussion: zoom-in on SMEs

12.30 *Lunch break*
14.00 **Break-out sessions**

- Registry Lock - what’s new?
- How are we dealing with online fraud?
- Incentives (types of incentives, what works, what doesn’t)
- How can registries and registrars work together to face the changing domain landscape?

15.00 **Plenary: outcome of break-out session discussions**
15.30 *Coffee break*
16.00 **EU Policy Update**
16.00 **EThe future of the domain name industry – open mic sessione**
17.00 **End**

SARUNA AR CERT.LV KIBERDROŠĪBAS EKSPERTU GINTU MĀLKALNIETI

Mēs bieži piemirstam, ka sākotnēji, internets tika radīts, kā noslēgts tīkls. Tas nebija paredzēts publiskai lietošanai, bet gan konkrētām militārām ASV aizsardzības ministrijas izpētes vajadzībām. Cilvēki, kas jelkādā veidā fiziski tika klāt ierīcēm, kas pieslēgtas internetam, bija izgājuši skrupulozas pārbaudes – visa viņu darbība tika cītīgi kontrolēta un piefiksēta (datums, laiks, veiktās darbības). Būvējot internetu, neviens nesatraucās un neiedomājās, ka kāds nākotnē varētu izlikties par kādu citu. Vienkārši nebija vajadzības pēc drošības pasākumiem.

Gints Mālkalnietis, CERT.LV

Diemžēl mūsdienās spēles noteikumi ir radikāli mainījušies. Tīkls ir vērienīgi izaudzis, pie tā var piekļūt jebkurš, kas vienkārši nopērk mobilo telefonu vai kādu citu mobilo iekārtu un mēs nezinām nedz to, kas tā ir par personu, nedz ko šī persona grasās ar šo piekļuvi darīt. Tādēļ internets tika, tiek un tiks apbūvēts ar dažādiem drošības slāņiem un rīkiem. Ko tas nozīmē mūsdienu uzņēmējam? Lielām kompānijām ir savi IT drošības speciālisti vai pat komandas, kuru tiešais pienākums ir rūpēties par IT drošību, taču ko darīt mazajam un vidējam uzņēmumam?

CERT.LV kiberdrošības eksperts Gints Mālkalnietis, ikdienā strādājot un analizējot Latvijas kibertelpā notiekošo, ir novērojis, ka pēdējo divu gadu laikā Latvijā ir ievērojami pieaudzis kiber-incidentos cietušo skaits tieši mazo un vidējo uzņēmumu vidū. Lai šo bēdīgo statistiku uzlabotu, ir svarīgi runāt un atgādināt par vienkāršām, taču iedarbīgām ikdienas kiber-higēnas un digitālās etiķetes darbībām, kas var izglābt no interneta draudiem un visbiežākajiem uzņēmēju klupšanas akmeņiem.

Kopš maija CERT.LV kopā ar NIC un LTRK uzrunā un iepazīstina uzņēmējus ar kiberdrošības aktualitātēm, uzstājoties semināru ciklā "KĀ UZŅĒMĒJAM VIEGLI (ne) PAZAUDĒT NAUDU KIBERTELPĀ".

KĀDAS IR AKTUĀLĀKĀS MAZO UN VIDĒJO UZŅĒMUMU KIBERDROŠĪBAS PROBLĒMAS?

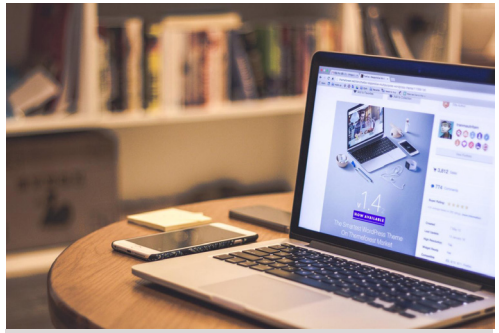
Noteikti e-pasts! Vēl joprojām pastāv priekšstats: ja saņemu viltus e-pastu kolēģa vārdā, tātad viņa dators ir uzlauzts. Taču tā visbiežāk nav. E-pasta protokols ir ļoti naivs un primitīvs. Tas neveic pārbaudi, vai sūtītājs ir norādījis sevi korekti. Jebkurš var nosaukt sevi kā vēlas, norādot svešu adresi sūtītāja "From" laukā.

> **Problēma slēpjas faktā, ka e-pasts mūsdienās ir kļuvis ne tikai par saziņas rīku, bet par nopietnu biznesa instrumentu. Uzņēmumi pārskaita vērienīgus finanšu līdzekļus uz e-pastā norādīto pieprasījumu pamata, lai gan e-pasta nosaukumu un tekstu ir ļoti viegli viltot.**

Šāda prakse vēl joprojām strādā, tādēļ uzņēmēji zaudē naudu. Latvijā ir zināms piemērs, kad kiberuzbrukuma rezultātā uzņēmums pārskaitīja tuvu 1 miljonam EUR uz nepareizu kontu. Šādos gadījumos nepieciešams reaģēt nekavējoties un informēt par šo incidentu CERT.LV un policiju. Latvijā ir bijuši gadījumi, kad ar bankas palīdzību, tomēr izdodas pārskaitījumu apstādināt, taču ne visos gadījumos tas ir iespējams.

Lai viltotu e-pasta rēķinu, uzbrucējiem pilnīgi pietiek piekļūt pie viena e-pasta sūtītāja vai saņēmēja pastkastītes, lai saprastu, ka tiks veikts kāds vērienīgs darījums. Uzbrucējs iejaucas, izmantojot specifiskus domēna vārdus, kas tiek veidoti līdzīgi oriģināliem (piemēram ar drukas kļūdām), dažreiz pat ne tik līdzīgus. Cilvēki nepievērš uzmanību vai nepamana, ka, piemēram, ierastā janis@internet.lv vietā saņem e-pastu no janis@intemet.lv (r+n tiek aizvietots ar m), vai arī GMAIL vietā tiek izmantots YAHOO. Sevišķi, ja e-pasta tekstā tiek izmantoti kādi iepriekšējās sarakstes citāti ar nevainīgu norādi, ka naudas pārskaitījums ir jāveic uz citu kontu.

Izmantojot e-pastu, tiek izsūtīti tā dēvētie "pikšķerēšanas" e-pasti (phishing scam) ar mērķi iegūt jūsu tiešsaistes pakalpojumu kontu lietotāja datus. Arī šeit bieži vien uzbrucējs izmanto līdzīgus domēna vārdus vai to pašu vārdu tikai citā paplašinājumā, domēnā. Tādēļ uzņēmējiem un viņu darbiniekiem ir jābūt ļoti vērīgiem, no kā



KĀ UZŅĒMĒJAM VIEGLI (ne) PAZAUDĒT NAUDU KIBERTELPĀ

2019. gada 24. septembrī
plkst. 13:00 - 16:00
Valmieras integrētās bibliotēkas
2. stāva zālē, 217. telpā,
Valmierā

Reģistrējies līdz 23.septembrim ŠEIT vai
valmiera@chamber.lv
tel. 20264530
LTRK biedriem bez maksas

saņem e-pastu un kādu URL grasās spiest un apmeklēt.

KURAS NO E-PASTA DROŠĪBAS TEHNOLOĢIJĀM JŪS IETEIKTU IZMANTOT? KAS PALĪDZĒTU UZŅĒMĒJIEM IZVAIRĪTIES NO ŠĀDA VEIDA UZBRUKUMIEM?

E-pasta drošībai ir ieviestas vairākas tehnoloģijas DKIM, DMARC, SPF, kas ļauj digitāli parakstīt e-pastus un pārliecināties, ka e-pastus tiešām esat izsūtījuši Jūs. Vienīgi parakstīt jau Jūs varat, bet pārbaudīt tāpat nāksies saņēmējam, ja saņēmējs to nedara, tad drošība līdz galam nenostrādā. Ja Jūsu uzņēmums lieto DMARC, pievēršat uzmanību, vai paši pārbaudāt citu saņemtos parakstus. Taču šīs tehnoloģijas nepalīdz, ja uzbrucējs izmanto līdzīgu ("typo") domēna vārdu, vai to pašu nosaukumu citā paplašinājumā. Tādēļ lieli uzņēmumi un zīmoli kiberdrošības nolūkos mēdz reģistrēt un izmantot arī domēna vārdus ar izplatītākajām sava zīmola vai uzņēmuma nosaukuma drukas kļūdām, kā, piemēram, TWITTER ir reģistrējis ne vien twitter.com, bet arī twiter.com.

> **Ja vēlamies panākt pēc iespējas lielāku drošību, mēs nonākam līdz totālai pārbaudei – digitālie paraksti it visur! Sūtām tikai digitāli parakstītus dokumentus, un atļaujam grāmatvedei pārskaitīt naudu tikai uz digitāli parakstītu dokumentu pamata.**

VAI TAS NOZĪMĒ, KA KATRAM UZŅĒMUMAM IR NEPIECIEŠAMS SAVS IT DROŠĪBAS SPECIĀLISTS, KURŠ UZMANĪS UN IZGLĪTOS DARBINIEKUS PAR VISIEM IT RISKIEM?

Latvijā IT speciālistu nav daudz, labu IT speciālistu ir vēl mazāk. Maziem uzņēmumiem tīri objektīvi nepietiek, pirmkārt, finanses un, otrkārt, pašu speciālistu, tādēļ mazākiem uzņēmumiem labāk būtu šo pakalpojumu iegādāties kā ārpakalpojumu. Vēlams, lai izvēlētai organizācijai būtu labas atsauksmes un atbilstoši sertifikāti, kas apliecinātu viņu spēju kaut ko izdarīt. Es vairāk uzsvaru liktu uz labām atsauksmēm, kas bieži vien ir daudz svarīgākas par ziedošiem sertifikātiem.

Diemžēl novērtēt, cik labs vai slikts ir izvēlētais ārpakalpojumu sniedzējs, tā patiesi varēs tikai pēc laika. Svarīgi ir arī pašiem uzņēmējiem saprast, ko pieprasīt no ārpakalpojumu sniedzēja. Katram uzņēmumam sev vai savam ārpakalpojumu sniedzējam vajadzētu pajautāt:

1. **Kas veido, kur un kā tiek saglabātas rezerves kopijas man svarīgiem datiem?** Tas ir punkts numur viens, kas uzņēmumiem ir vissāpīgākais. Tie var būt grāmatvedības dati vai jel kas cits ar uzņēmuma darbības specifiku saistīts. Datu zudums var būt par pamatu uzņēmējdarbības pārtraukšanai. Dati pazūd dažādu iemeslu dēļ, tas var nebūt kiberuzbrukums, bet vienkārši zādzība, ugunsgrēks, citas nelaimes vai tehniskas problēmas, piemēram, ar datora cieto disku. Tie, kas vienu reizi jau ir "apdedzinājušies", vēlāk par šo jautājumu piedomā cītīgāk.
2. **Cik un kādas man ir datoru programmas un to licencēšanas statuss?** Šis ir nepieciešams, lai nerastos negaidīti jautājumi no VID un citām iestādēm par uzņēmumu datora nodrošinājumu.
3. **Kāds ir statuss antivīrusa programmai?** Kad tā ir pēdējo reizi atjaunota?
4. **Ja uzņēmumam ir tīmekļa vietne, jānoskaidro:**
   - **Kas, kad to ir izveidojis un atjauno, kur tā atrodas un kam ir pieeja?** Diemžēl mājaslapa nav statiska lieta, pat ja informāciju tajā netiek atjaunota. Mājaslapas, neskatoties uz to, ka izveidota ar Wordpress, ir jāatjaunina. Šo procesu, protams, var automatizēt, uzticot ārpakalpojumu uzturētājam.
   - **Kādi man ir domēna vārdi un kas ir to "īpašnieks", kurš var veikt izmaiņas?** Bieži vien mēs uzticam sava uzņēmuma domēna vārdu reģistrēšanu kādam tehniskajam darbiniekam, kurš vienkāršības labad to piereģistrē uz sava vārda. Kad darbinieks aiziet no darba, uzņēmums labākā gadījumā zaudē tikai kontroli pār savu domēna vārdu, ļaunākā - pašu domēna vārdu. Tas var būt liels trieciens uzņēmējdarbībai, īpaši ja komunikācija ar klientu notiek caur internetu.
5. **E-pasts - kas, kur to uztur, vai tiek veidotas rezerves kopijas?** Var izmantot arī mākoņ-risinājumus, tikai jāsaprot, cik tas uzņēmumam ir kritiski un kas tiks darīts, ja mākoņi "apgāzīsies". Kas paliks uzņēmuma datoros un kas nepaliks?

VAI DOMĒNA VĀRDA LIETOTĀJU PERSONAS DATU PUBLICĒŠANAS IEROBEŽOJUMI, KO PAREDZ PAAUGSTINĀTAS PERSONAS DATU AIZSARDZĪBAS PRASĪBAS (VDAR), SAREŽĢĪ KIBERNOZIEGUMU IZMEKLĒŠANU?

CERT.LV darbību sarežģī nevis tas, ka neredzam WHOIS, kura persona ir domēna vārda lietotājs, bet gan, ka lietotāji norāda nekorektu kontakta e-pasta adresi un telefona numuru. Akūtos gadījumos ir nepieciešams operatīvi personas informēt par radušos kiber-incidentu, kurā ir iesaistīts viņu domēna vārds un tīmekļa vietne. Protams, arī mitinātājam var būt sava lietotāja kontaktinformācija, taču diemžēl operatīvi un ātri šo informāciju mēs nevaram iegūt. Parasti personas nenorāda savu e-pasta adresi un telefona numuru, jo baidās no SPAM un reklāmas zvaniem. Tik slepeni rīkoties nevajag, jo praksē šo informāciju tāpat nākas izvietot, piemēram, mājaslapā, lai klienti ar Jums varētu sazināties. Nevar garantēt, ka arī kādā brīdī kāds datorvīruss no Jūsu sarakstes biedra datora adrešu grāmatiņas nenokopēs Jūsu e-pasta adresi.

> **Jebkura e-pasta adrese, kura tiek, reāli izmantota, var saskarties ar SPAM. Ir saprotams, ka lietotājs nevēlas saņemt savā e-pasta adresē reklāmas, bet ja netiks norādīta korekta kontaktinformācija, tad nevarēs arī ar Jums sakontaktēties tiešām svarīgos jautājumos. Tādēļ atgādinu, ka ir nepieciešams aktualizēt un norādīt korektu kontakta informāciju NIC, lai akūtos gadījumos drošības institūcijas, kā CERT.LV un policija, varētu ar Jums sazināties.**

KĀDU PADOMU JŪS SNIEGTU INTERNETA LIETOTĀJIEM UN TĪMEKĻA VIETŅU, E-VEIKALU VEIDOTĀJIEM, LAI IKVIENS JUSTOS DROŠĀK TIEŠSAISTĒ?

Neglabāt vairāk datus pie sevis kā nepieciešams! Ja uzņēmums glabā paroles, tās mūsdienās nav pieļaujams glabāt atklātā tekstā. Ja ir novecojusi sistēma, kurā tā tiek darīts, tā ir jālabo. Pat ja noplūdušo datu apjoms nav liels, tāpat tā ir saruna ar Datu valsts inspekciju par to, kā un kādēļ šie dati ir glabāti. Labāk laicīgi parūpēties, lai saglabātie dati nevarētu tikt izmantoti ārpus sistēmas.

Ja ir iespēja, visās tiešsaistes autentifikācijās izmantojam kaut ko vairāk par vienu paroli (divu faktoru autentifikāciju) vai vismaz piedāvājiet cilvēkiem tādu iespēju, teiksim vienreiz lietojamās paroles vai Google autentifikatoru. Tas ievērojami palielina drošību.

SPILGTĀKĀ .LV REĢISTRATŪRA LATVIJĀ!

Katrā .LV Reģistratūru avīzes numurā lasītājiem sniedzam ieskatu par kādu Latvijas .LV Reģistratūru. Tas ir veids, kā varam izcelt reģistratūras, ar kurām ir izveidojusies laba sadarbība, kuras ir aktīvākas vai straujāk augošās, un pateikt paldies par sadarbību, kuru mēs tik augstu novērtējam.

REGISTAR – SIA PRO WEB

Mājaslapu izveides un uzturēšanas pakalpojumu sniedzējs SIA Pro Web par .LV Reģistratūru kļuva 2010.gada martā. Sākotnēji piedzīvots straujšs domēna vārdu skaita pieaugums – dažkārt pat teju 50% gadā, vēlāk – uzņēmums sevi pierāda kā stabilu uz attīstību vērstu uzņēmumu. NIC vienmēr priecājas par uzņēmumiem, kuriem ir svarīga to ilgtspējība, kuri rūpējas par saviem klientiem un arvien attīstās. Tieši tādēļ šoreiz kā spilgtākās Latvijas reģistratūras titula RegiSTAR ieguvēju esam izvēlējušies tieši SIA Pro Web.

Uzņēmums "Pro Web" nodarbojas ar mājas lapu izveidi un hostinga pakalpojuma sniegšanu jau kopš 2005.gada sākuma. Pateicoties jaunākajām tehnoloģijām un optiskā tīkla ātrumam, Pro Web var nodrošināt kvalitatīvu mājas lapas izvietošanu. 14 gadu laikā uzņēmums ir guvis lielu pieredzi mājas lapu izvietošanā, nodrošinot pakalpojumam kvalitāti un garantiju.

Ar ko Jums asociējas .LV?

Galvenā asociācija ir piederība Latvijai un atpazīstamība vietējā tirgū.

Kāda ir Jūsu panākumu atslēga?

Visa pamatā ir rūpes par pakalpojuma pieejamību un ātrdarbību. Tāpat arī mūsu klienti augstu novērtē daudzpusīgo tehnisko atbalstu, jo mūsdienu tehnoloģiju pasaulē klientiem nākas saskarties ar dažādiem izaicinājumiem - sākot ar epasta konfigurāciju viedierīcēs un beidzot ar mājas lapas koda pilnveidošanu.

Kā Jūs vērtējat sadarbību ar NIC?

Pozitīva sadarbība ar NIC jau ir izveidojusies kopš 2005.gada. Pa šiem laikiem ir daudz kas īstenots no NIC puses, lai savstarpējā sadarbība būtu veiksmīga un kā visaugstāk novērtētāko varām minēt Reģistra-Reģistratūras modeļa ieviešanu.

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	★★★
Dalība NIC projektos	★★

"Mūsu prioritāte – apmierināts klients, tāpēc pievēršam lielu uzmanību mājas lapas izvietošanas kvalitātei, kā arī darbinieku izglītošanai."

SIA PRO WEB

SPILGTĀKĀ REĢISTRATŪRA LATVIJĀ

.LV

RegiStar 2019

SKAITĻI UN FAKTI

124 283

Kopējais reģistrēto .LV domēna vārdu skaits*

* (01.09.2019.)

354 M

Kopējais domēna vārdu skaits pasaulē*

* (CENTR statistika)

75 890

Kopējais .LV reģistrētāju / lietotāju skaits, no kuriem:

30 941 fiziskas personas

44 949 organizācijas

Visvairāk .LV lietotāju ir

34

gadu jauni

157

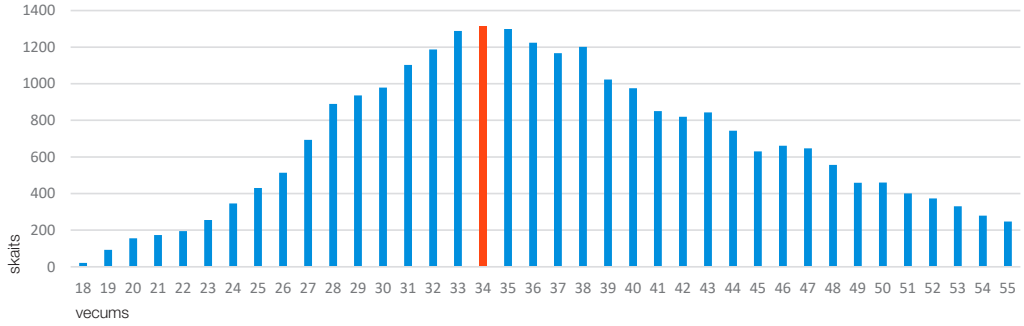
Kopējais .LV Reģistratūru skaits

2019. gadā noslēgti līgumi ar:

16 Ārzemju reģistratūrām

9 Latvijas reģistratūrām

LIETOTĀJU SADALĪJUMS PĒC VECUMA



DOMĒNA VĀRDU SKAITS PILSĒTĀS UN NOVADOS: