



GERZIC & Associates



ANALIZA BEZBEDNOSTI NACIONALNOG DOMENA

LUKA GERZIĆ

MILOŠ MARČETA

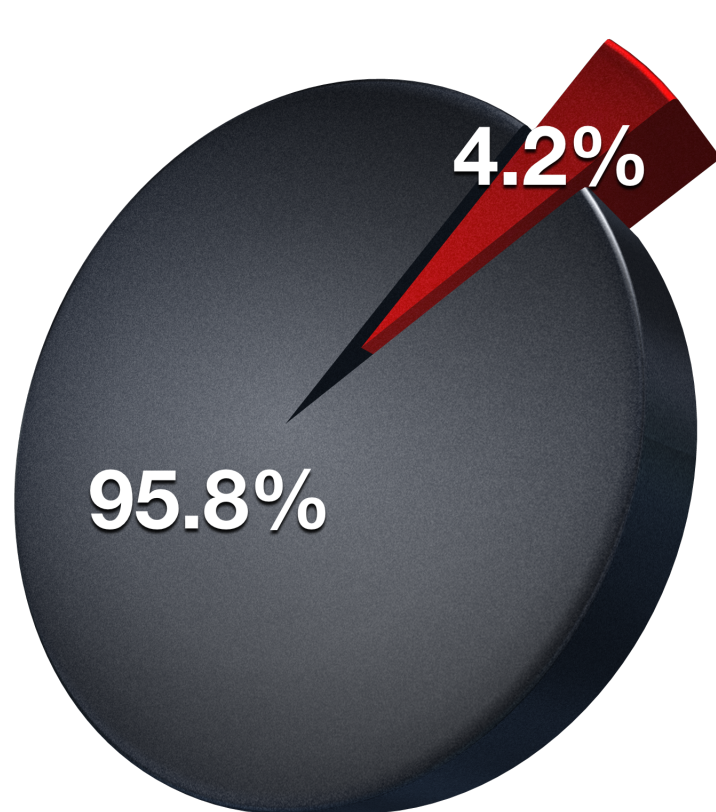
BEOGRAD, 2014/10/29

SRBIJA NA INTERNETU

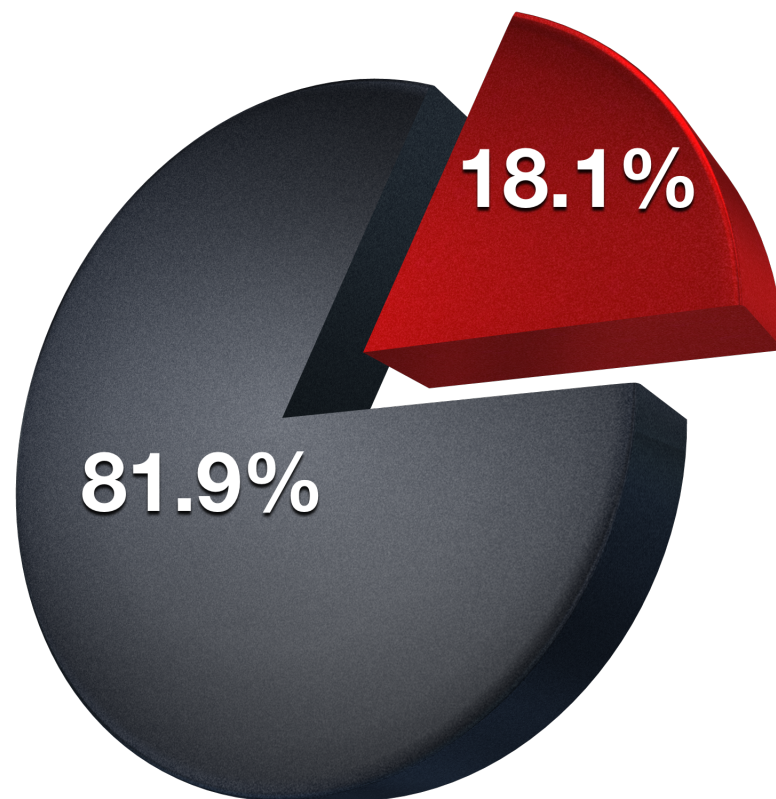
- Internet u Srbiji svakodnevno koristi **2,85 mil.** korisnika*
- **1,3 mil.** korisnika koristi e-servise javne uprave*
- **1,16 mil.** korisnika kupuje/prodaje preko Interneta*
- **28,3 mil.** dinara građani Srbije prosečno dnevno potroše preko Interneta ***
- **99%** preduzeća koristi Internet*
- **40** Ovlašćenih registara nacionalnog domena
- **86,291** registrovanih Internet domena (.rs + .cpб)**

AKTIVNI SERVISI - DNS, E-MAIL, WEB

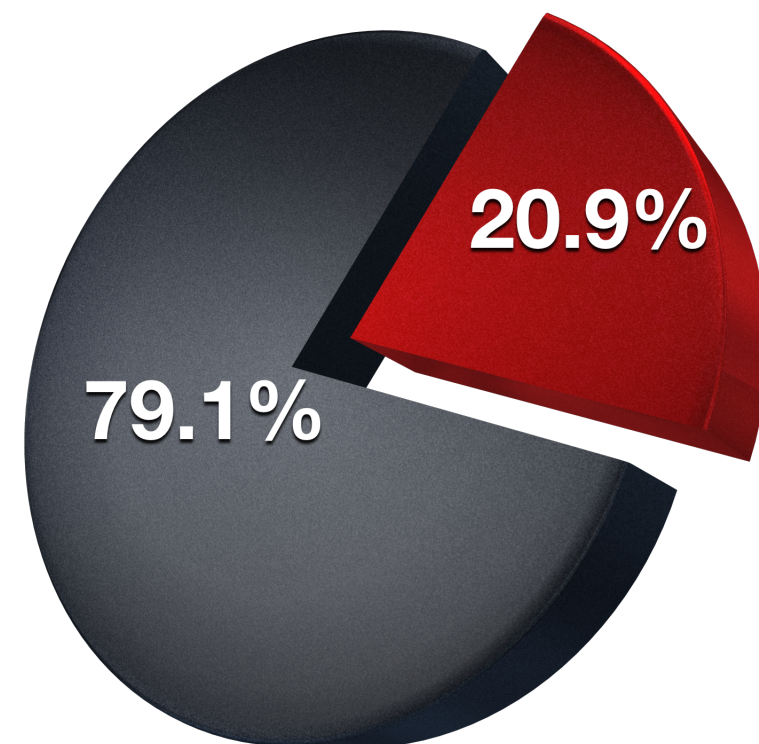
Svi domeni, bilo gde



● Ima DNS
● Nema DNS



● Ima MX
● Nema MX

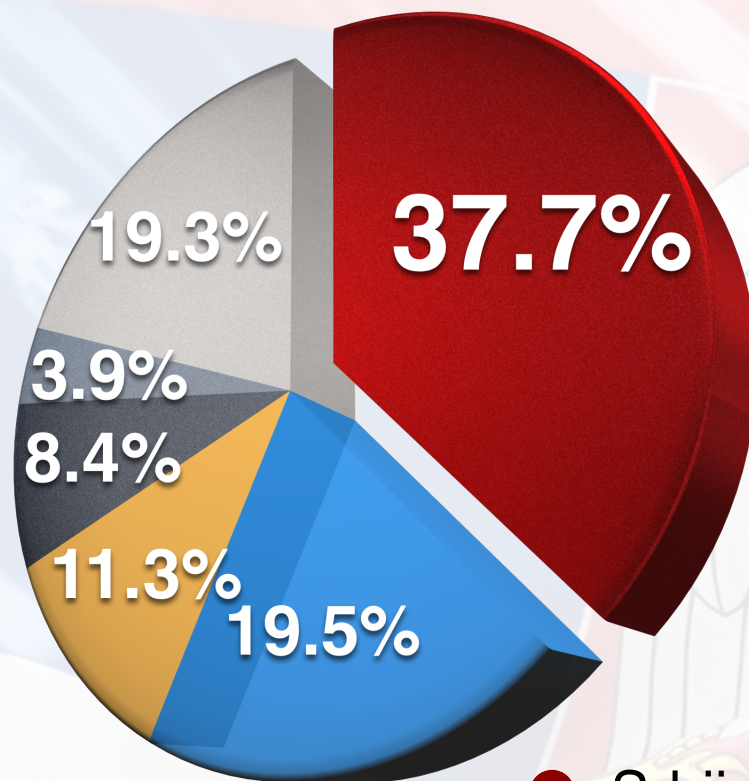


● Ima web servis
● Nema web servis *

GDE SRBIJA DRŽI SVOJ SADRŽAJ

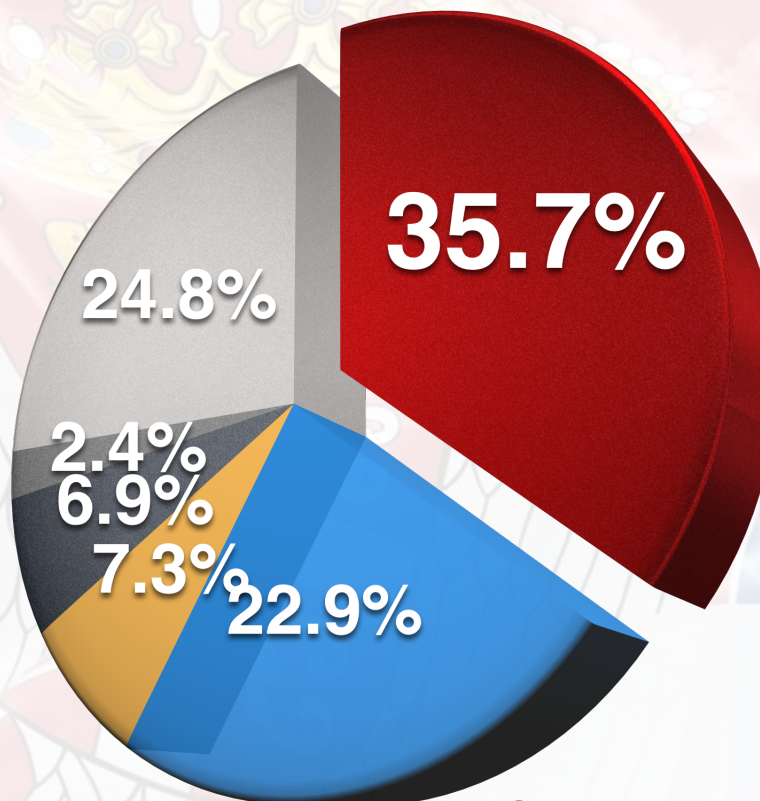
Svi domeni, bilo gde

DNS



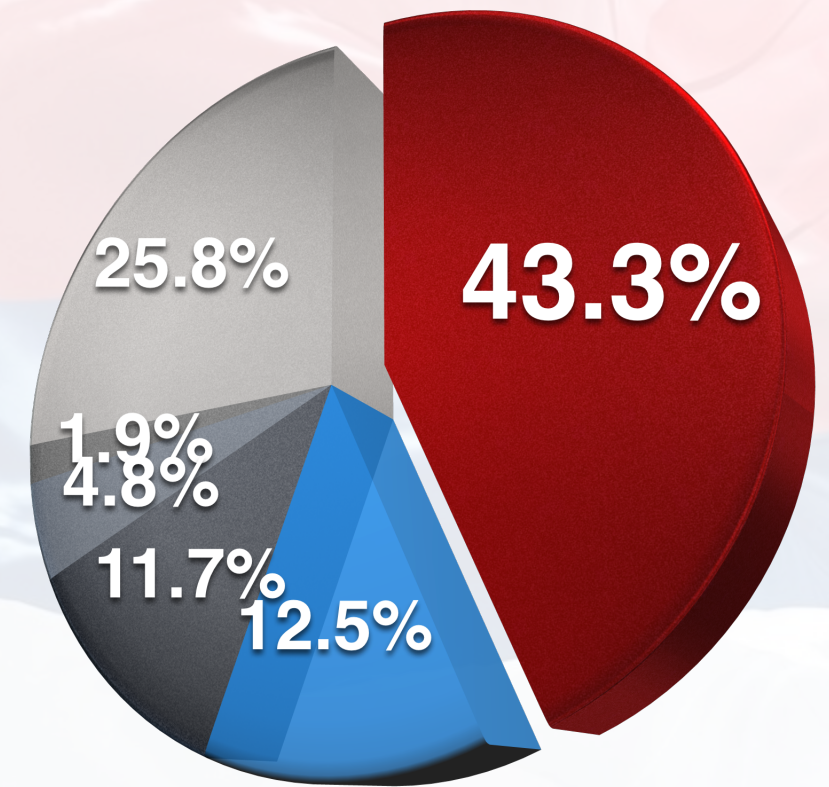
- Srbija
- SAD
- Švedska
- Nemačka
- Velika Britanija
- Ostali

E-mail



- Srbija
- SAD
- Švedska
- Nemačka
- Holandija
- Ostali

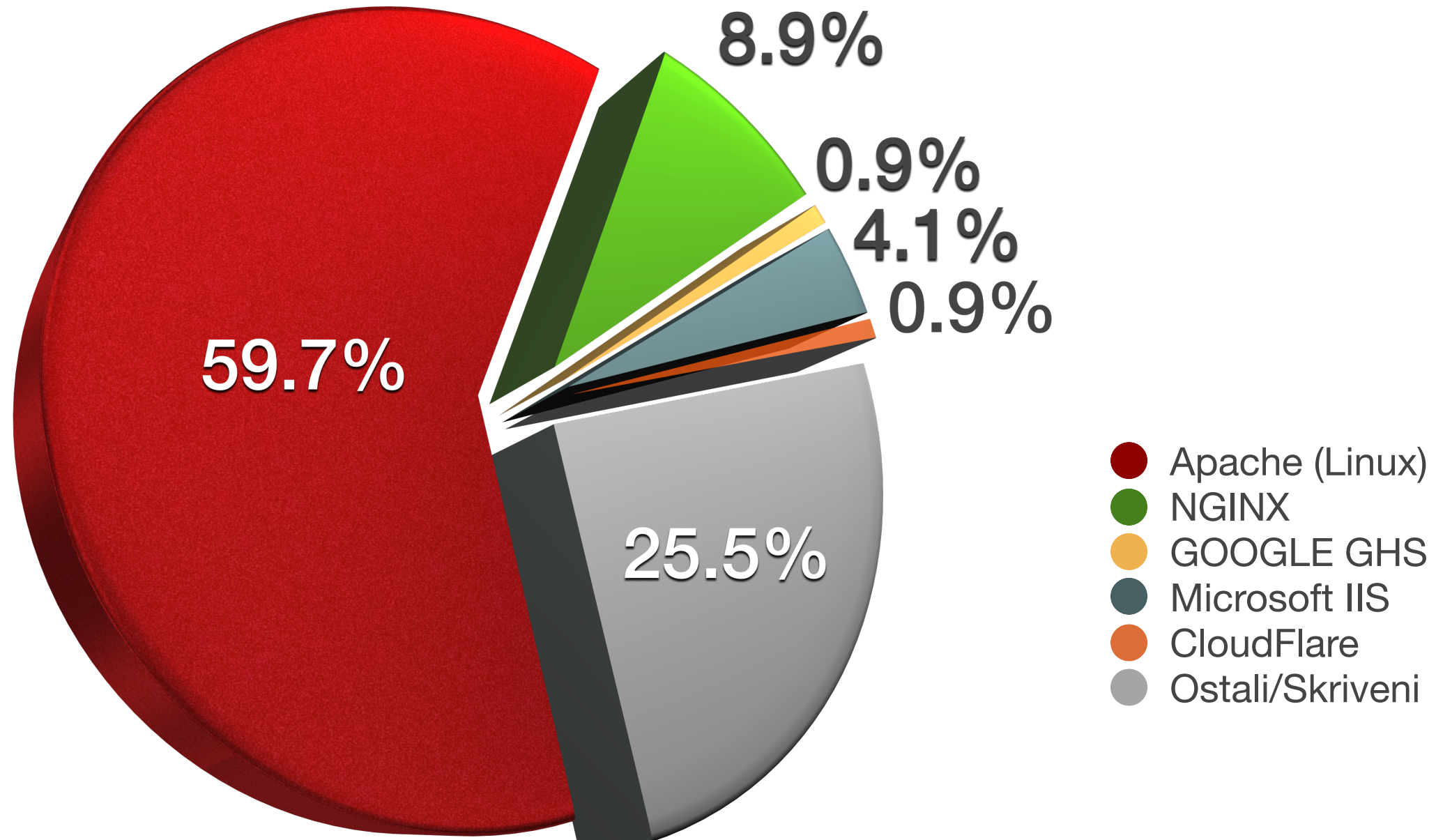
Web



- Srbija
- SAD
- Švedska
- Nemačka
- Holandija
- Francuska
- Ostali

KOM WEB SERVERU VERUJU SRBI

Svi domeni, bilo gde



KAKO FUNKCIONIŠE ENKRIPCIJA?



KAKO FUNKCIONIŠE ENKRIPCIJA?

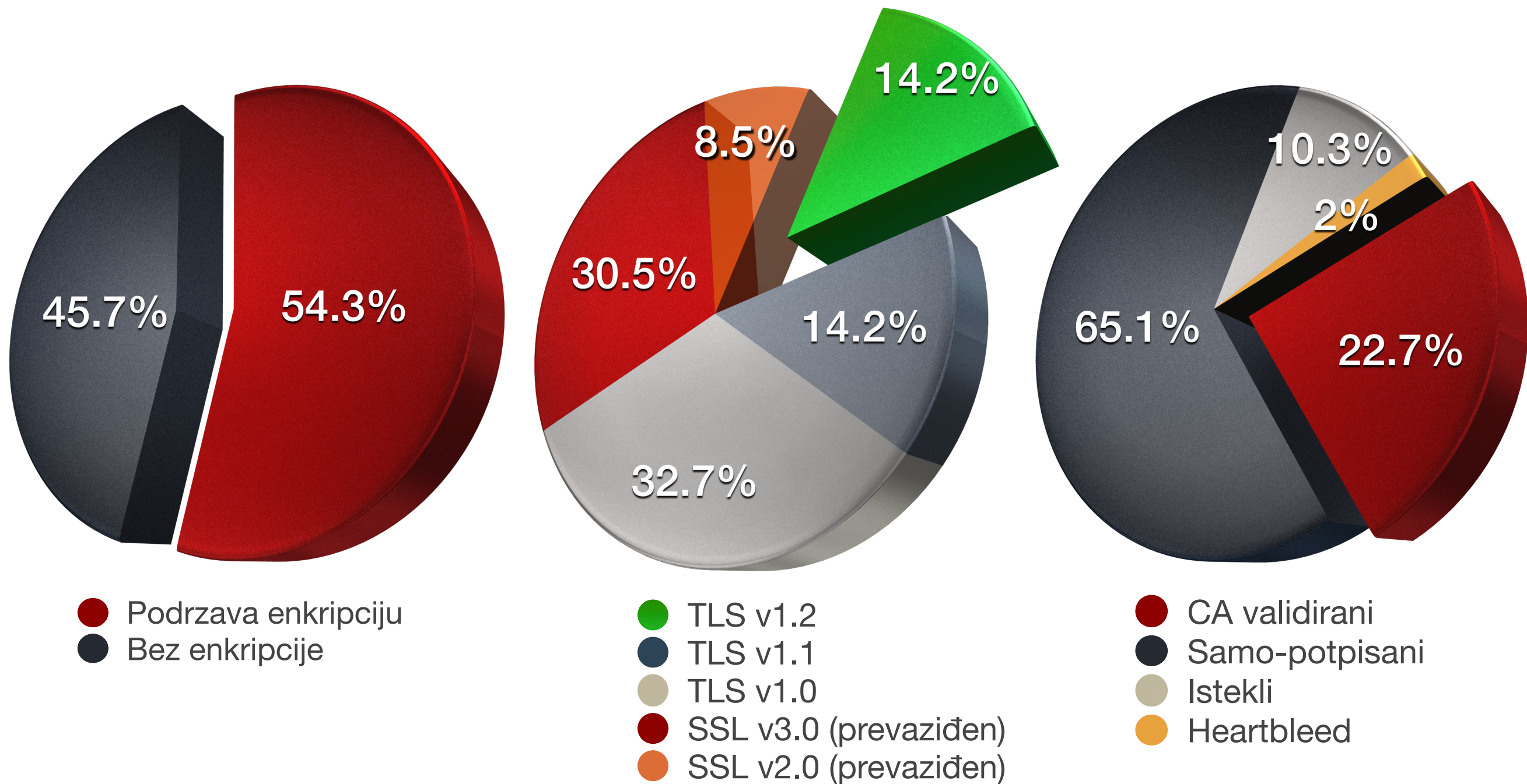


ZAŠTO BRINUTI?

- Nemam šta da krijem, nisam uradio ništa loše!
- Da li želite da prosledite svoj JMBG svakom?
- Da li želite da još neko može da čita vašu email poštu?
- Da li želite da svako zna da ste baš Vi ostavili neki politički komentar?
- Da li želite da svako ima uvid u vaš zdravstveni karton?
- Da li želite da svako ima uvid u vaš bankovni račun?

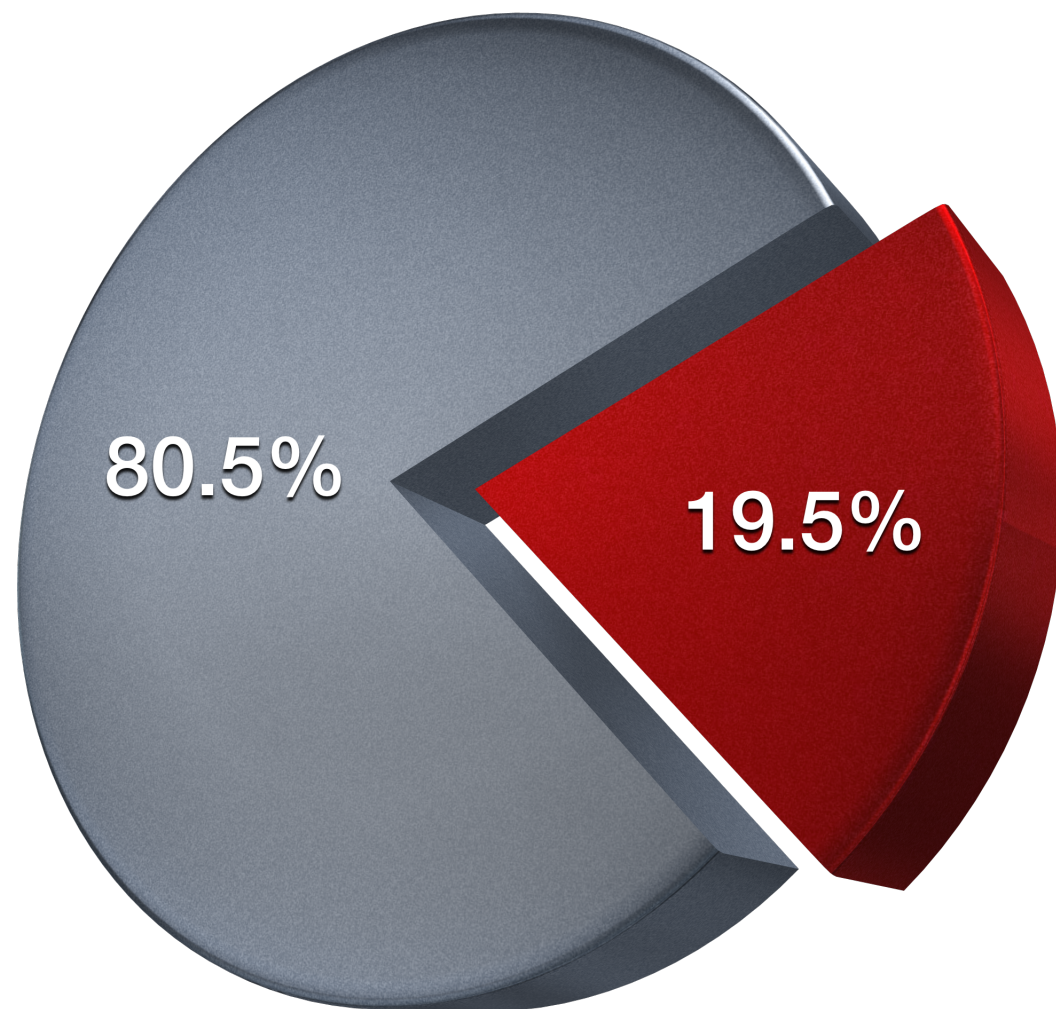
ENKRIPCJA WEB SERVISA U SRBIJI

Domeni, samo u Srbiji

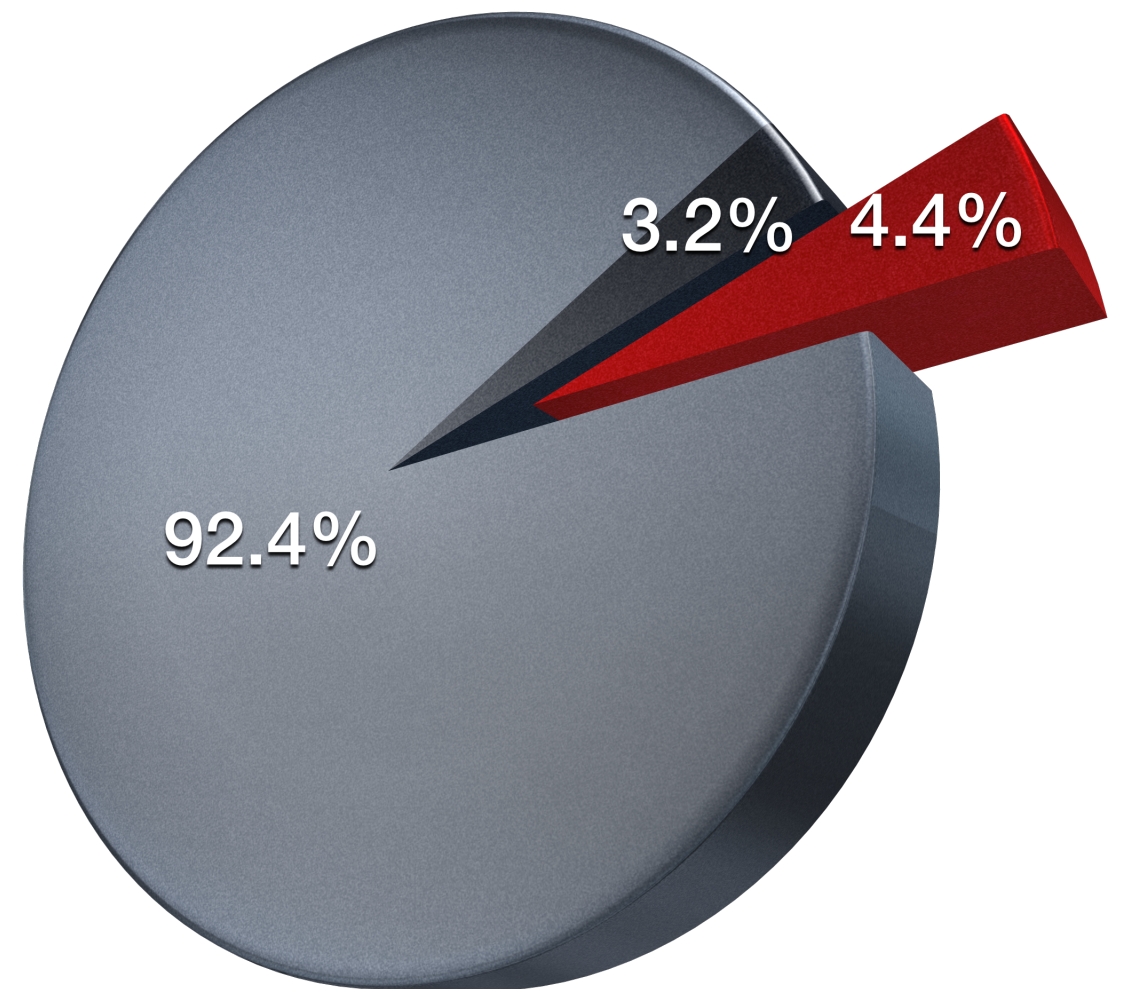


ENKRIPCJA WEB SERVISA U SRBIJI

Domeni, samo u Srbiji



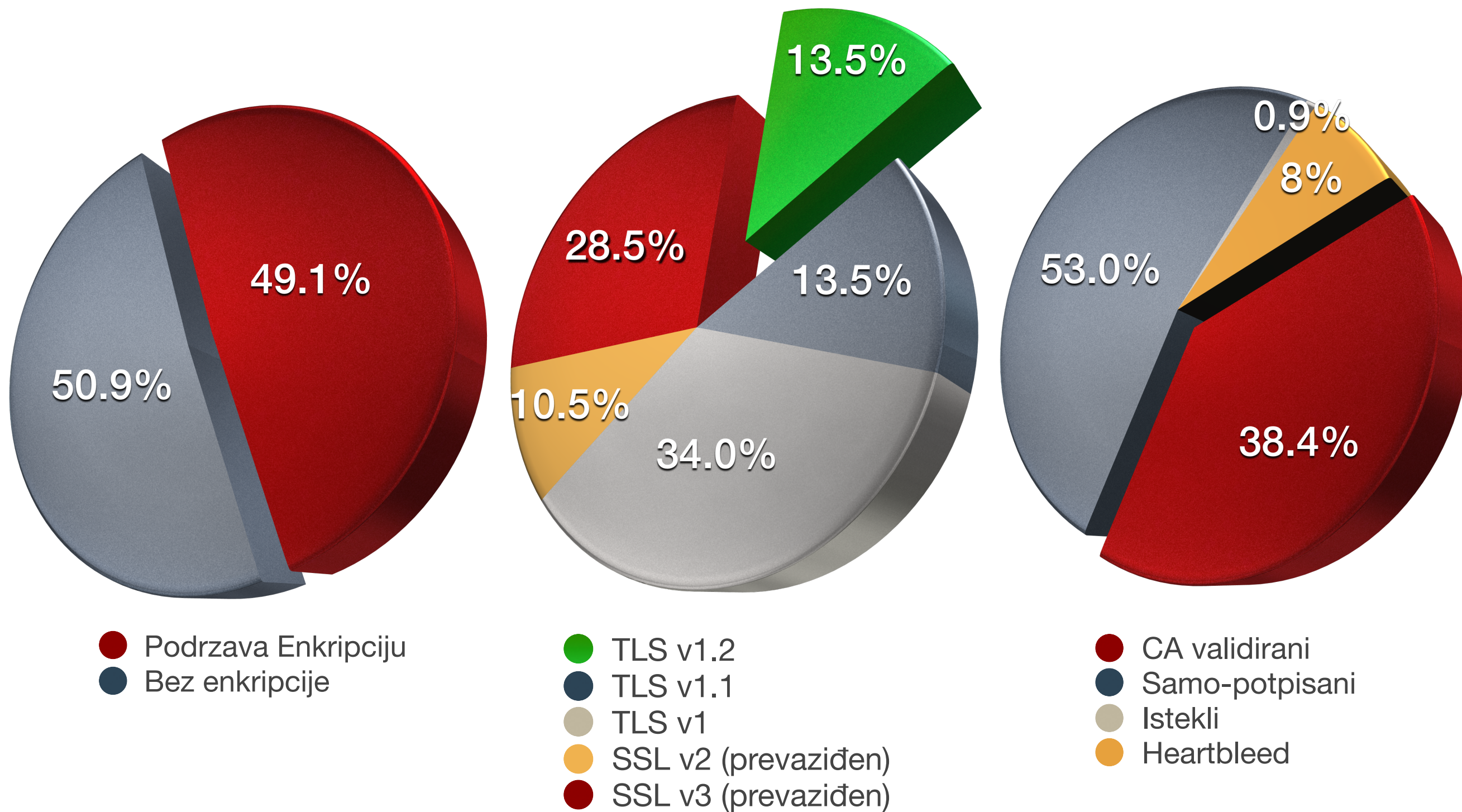
● Visok nivo ● Nizak nivo
Algoritmi šifrovanja podataka



● SHA256 ● SHA1 ● MD5
Algoritam potpisa

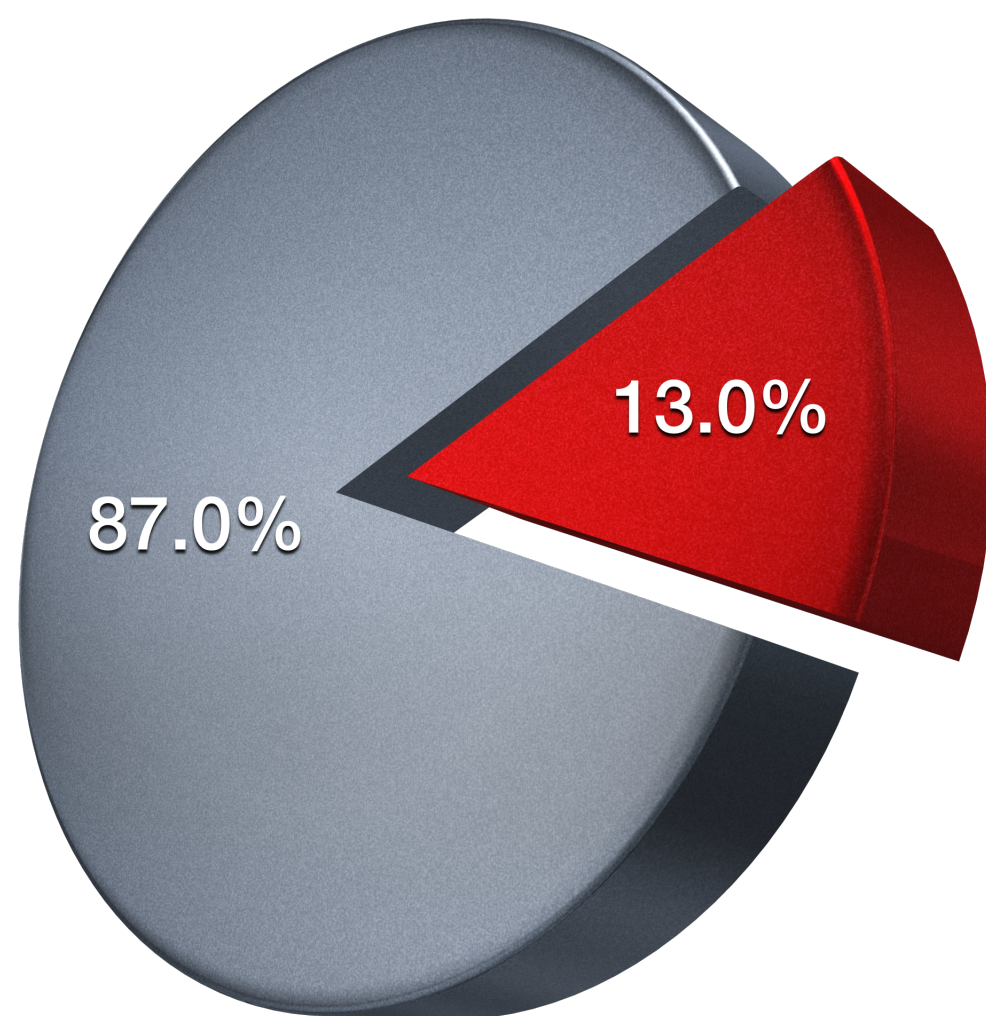
ENKRIPCJA SMTP SERVISA U SRBIJI

Domeni, samo u Srbiji

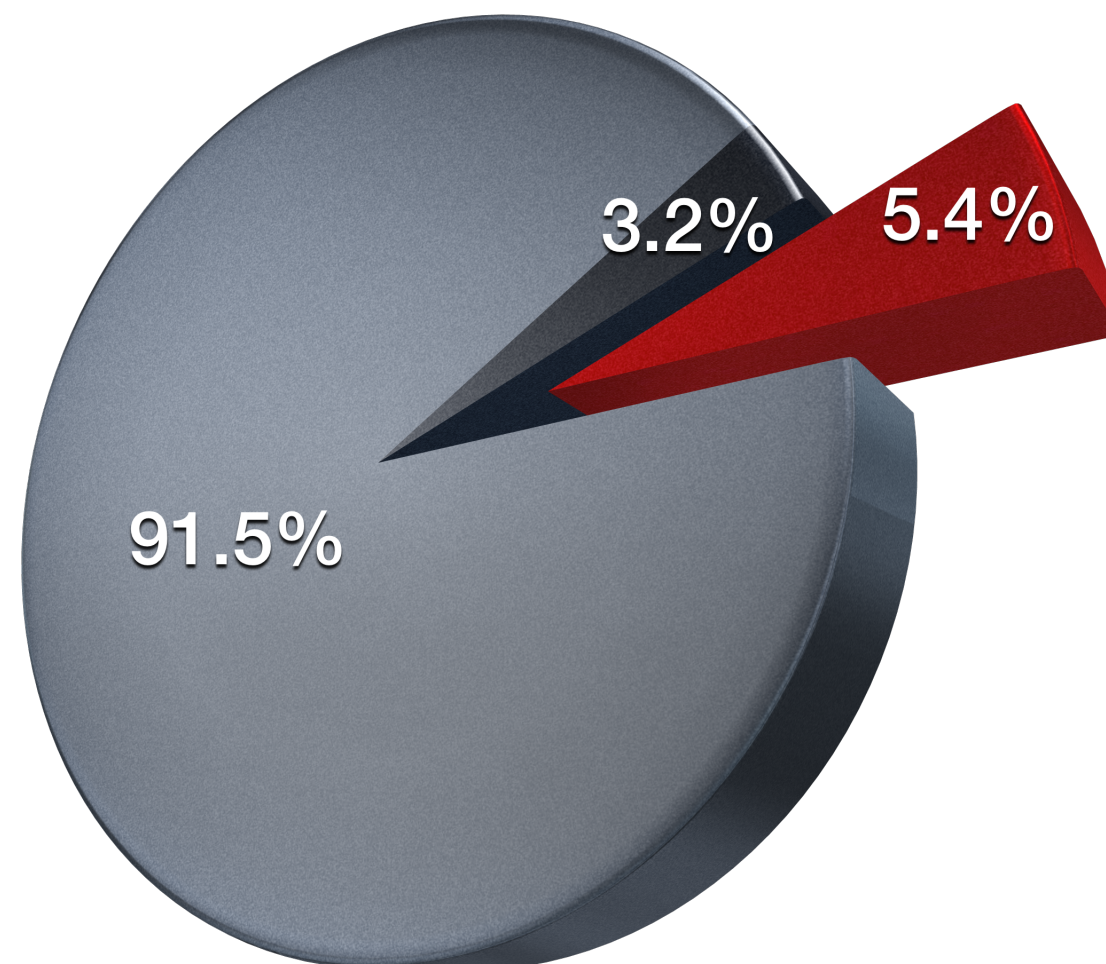


ENKRIPCJA SMTP SERVISA U SRBIJI

Domeni, samo u Srbiji



● Visok nivo ● Nizak nivo
Algoritmi šifrovanja podataka



● SHA256 ● SHA1 ● MD5
Algoritam potpisa

SRBIJA NA INTERNETU - NASTAVAK

- Od Top20 sajtova u Srbiji (***), **jedan** sajt ima aktivan HTTPS za posetioce
- Od 40 ovlašćenih registara Internet domena Srbije, **13 (32,5%)** ima validan CA SSL, a samo 1 ima HSTS aktivan
- Samo 2 (dva) domena u Srbiji imaju HSTS aktivan (0.002%**)
- Od skeniranih 101,293 WiFi uređaja na teritoriji Beograda **88,02%** ima podešenu zaštitu *

PREPORUCENA PODEŠAVANJA

Latest browsers: Firefox 27, Chrome 22, IE 11, Opera 14, Safari 7, Android 4.4, Java 8

Ciphersuite:

ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
DHE-RSA-AES128-GCM-SHA256
DHE-DSS-AES128-GCM-SHA256
kEDH+AESGCM
ECDHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA
ECDHE-ECDSA-AES128-SHA
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA
DHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA
DHE-DSS-AES128-SHA256
DHE-RSA-AES256-SHA256
DHE-DSS-AES256-SHA
DHE-RSA-AES256-SHA
!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

Versions: TLSv1.1, TLSv1.2

RSA key size: 2048

DH Parameter size: 2048

Elliptic curves: secp256r1, secp384r1, secp521r1

Certificate signature: SHA-256

HSTS obavezno!

HVALA NA PAŽNJI, PITANJA?



www.gerzic.com