Automatizacija provjere ranjivosti u mreži CARNeta

Marko Stanec
CARNet – odjel za Nacionalni CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Što je provjera ranjivosti?

- Postupak identifikacije poznatih ranjivosti računalnih sustava i mreža
- Korištenje specijaliziranih alata
- Analiza dobivenih rezultata
- Generiranje izvještaja

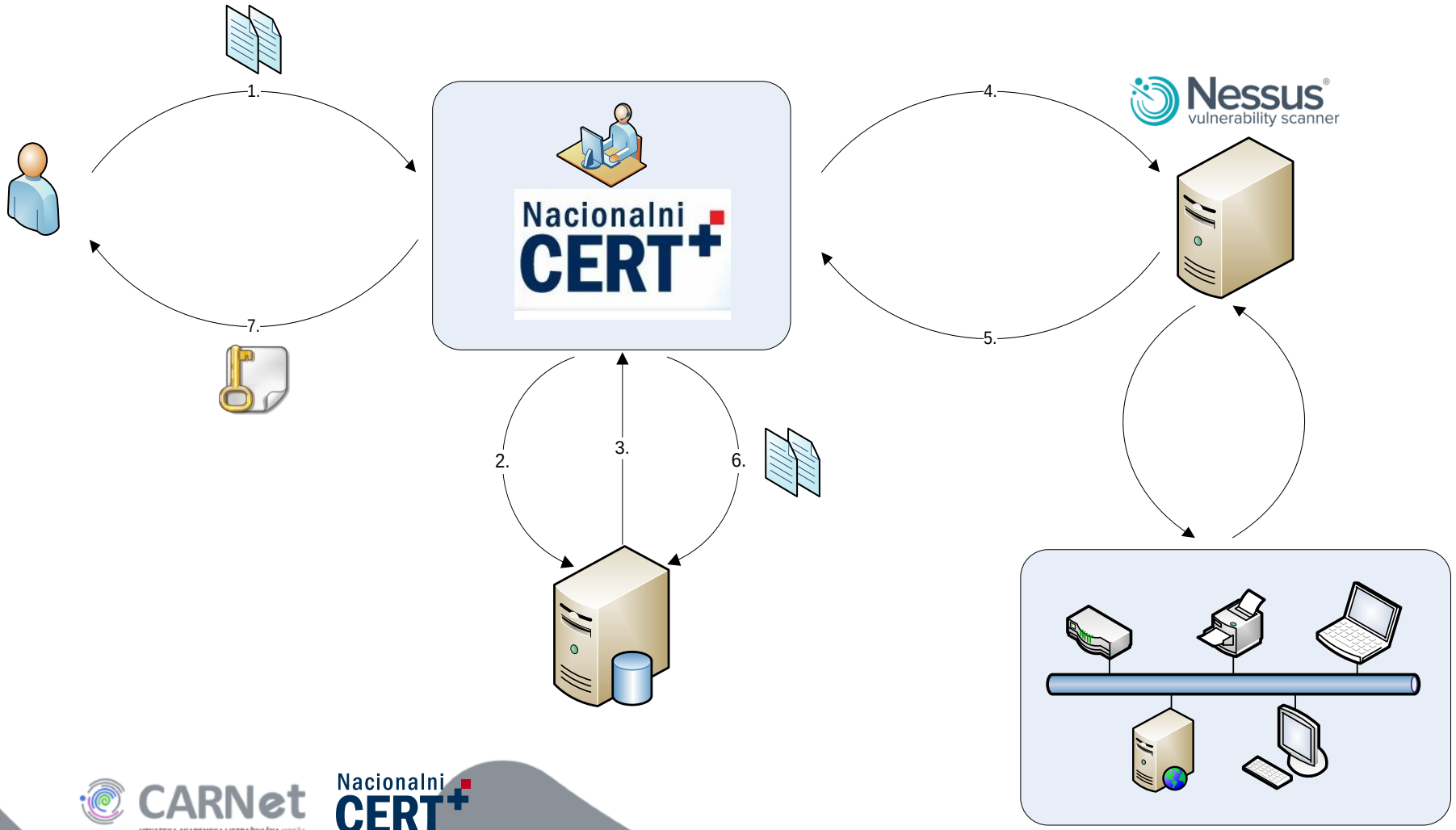
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Provjera ranjivosti u CARNetu

- Periodične provjere na zahtjev ustanova članica
- Korištenje alata Nessus®
- Broj ustanova: 59
- Broj provjera mjesečno: ~20

Shematski prikaz postupka provjere ranjivosti



Automatizacija provjere ranjivosti – ideja

- Opsežno skeniranje računalnih mreža svih ustanova članica CARNeta
- Sve punopravne članice CARNeta spojene stalnom vezom
- Rezultate poslati ustanovama na uvid
- Uvid u sigurnosno stanje mreže

Automatizacija provjere ranjivosti – razlog

- Zašto?
  - Utvrđivanje sigurnosnog stanja CARNet mreže
  - Unaprjeđenje sigurnosti CARNet mreže
  - U skladu sa CDA 0035 - Odluka o prihvatljivom korištenju CARNet mreže
- Kako?
  - Nessus® Vulnerability Scanner + NCERT alati
  - Periodičko obavljanje sigurnosnih provjera

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Automatizacija provjere ranjivosti – faze izvođenja

- Priprema podataka
- Nessus®
- SPORt
- Informiranje i distribucija rezultata

Priprema podataka

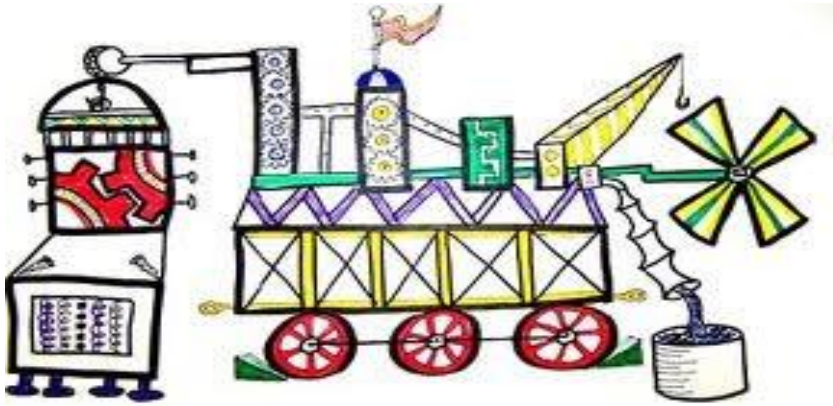
- Dizajn modela baze podataka
- Export „sirovih” podataka iz SZC-NOC baze
- Izrada skripte za obradu „sirovih” podataka i unos u SPORt:
  - Grupiranje ustanova, IP raspona, kontakt osoba
- Izdvajanje korisnika usluge Provjera ranjivosti i CARNetovih uređaja

Automatizacija Nessusa®

- Nessus® 5.0 REST protokol
- nessusxmlrpc
  - Python modul za automatiziranje poslova
  - prilagođen i proširen
- Automatizirano:
  - Pokretanje skenova
  - Preuzimanje izvještaja u PDF formatu

Sustav za Pohranu, Obradu i Preuzimanje Rezultata Opsežnog Skeniranja Mreže a.k.a. SPORt

- Web sučelje za pregled i dohvaćanje rezultata provjere
- Implementiran AAI@EduHR SSO mehanizam
- Omogućeno dohvaćanje izvještaja samo tehničkim osobama na ustanovi:
  - Administrator resursa/imenika
  - CARNet sistem inženjer
  - Zakonski predstavnik
- Statistički pregled rezultata



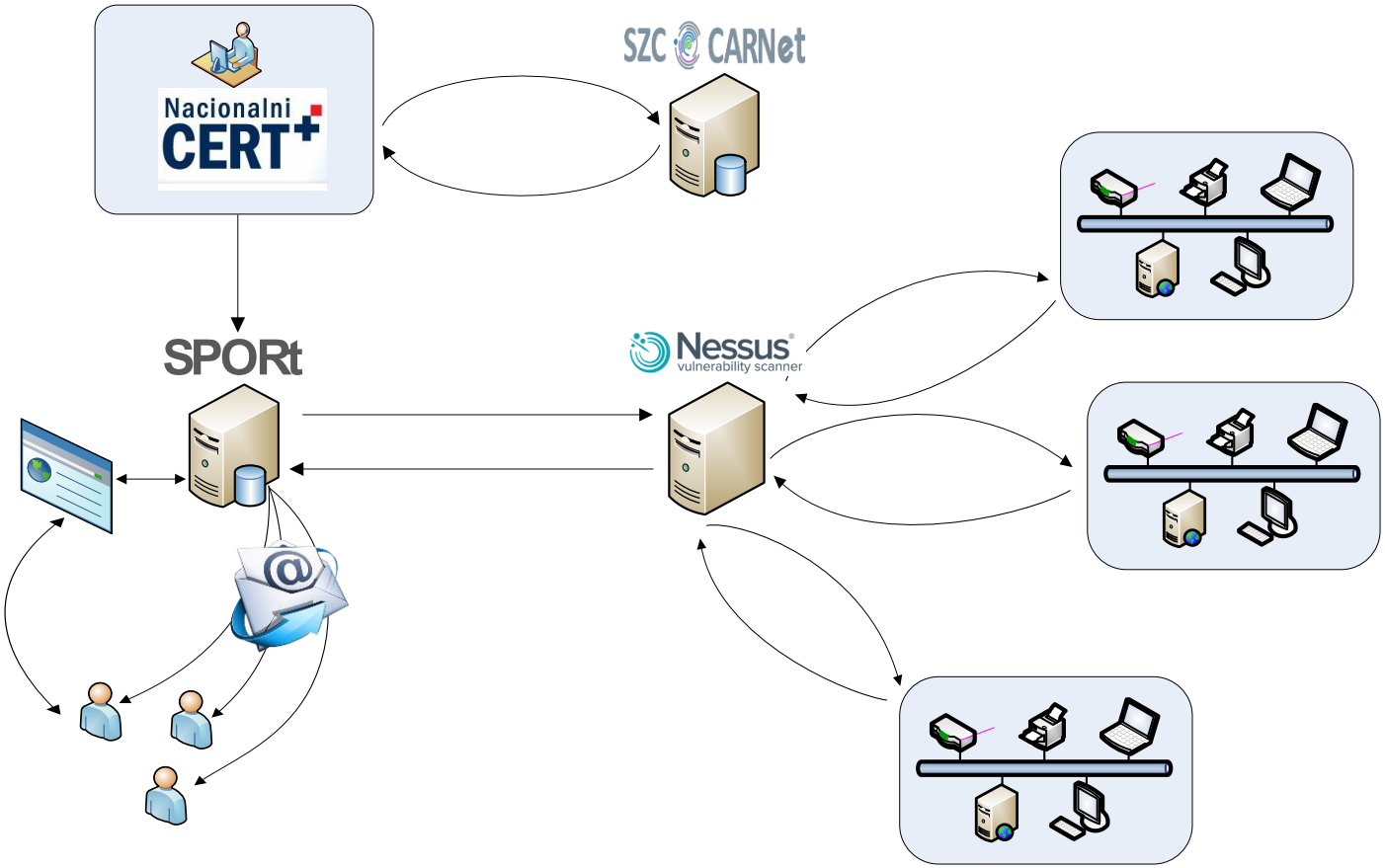
CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

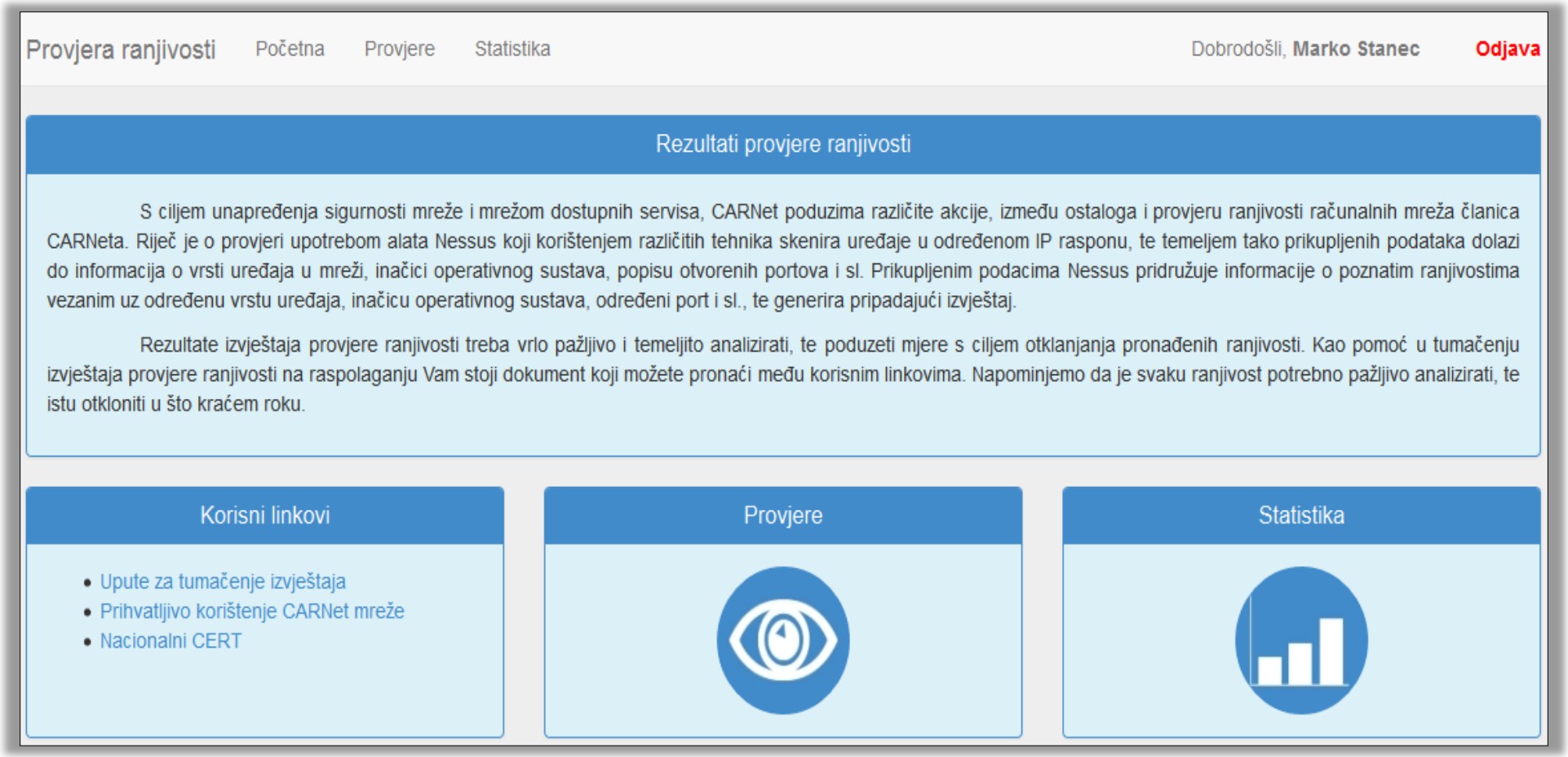
Informairanje i distribucija rezultata

- Automatizirano:
  - slanje obavijesti o planiranoj akciji mailom odgovornim osobama na ustanovi
  - slanje uputa kako preuzeti izvještaj po završetku provjere
- Izrađena uputa za tumačenje izvještaja

Shematski prikaz opsežnog skeniranja CARNet mreže



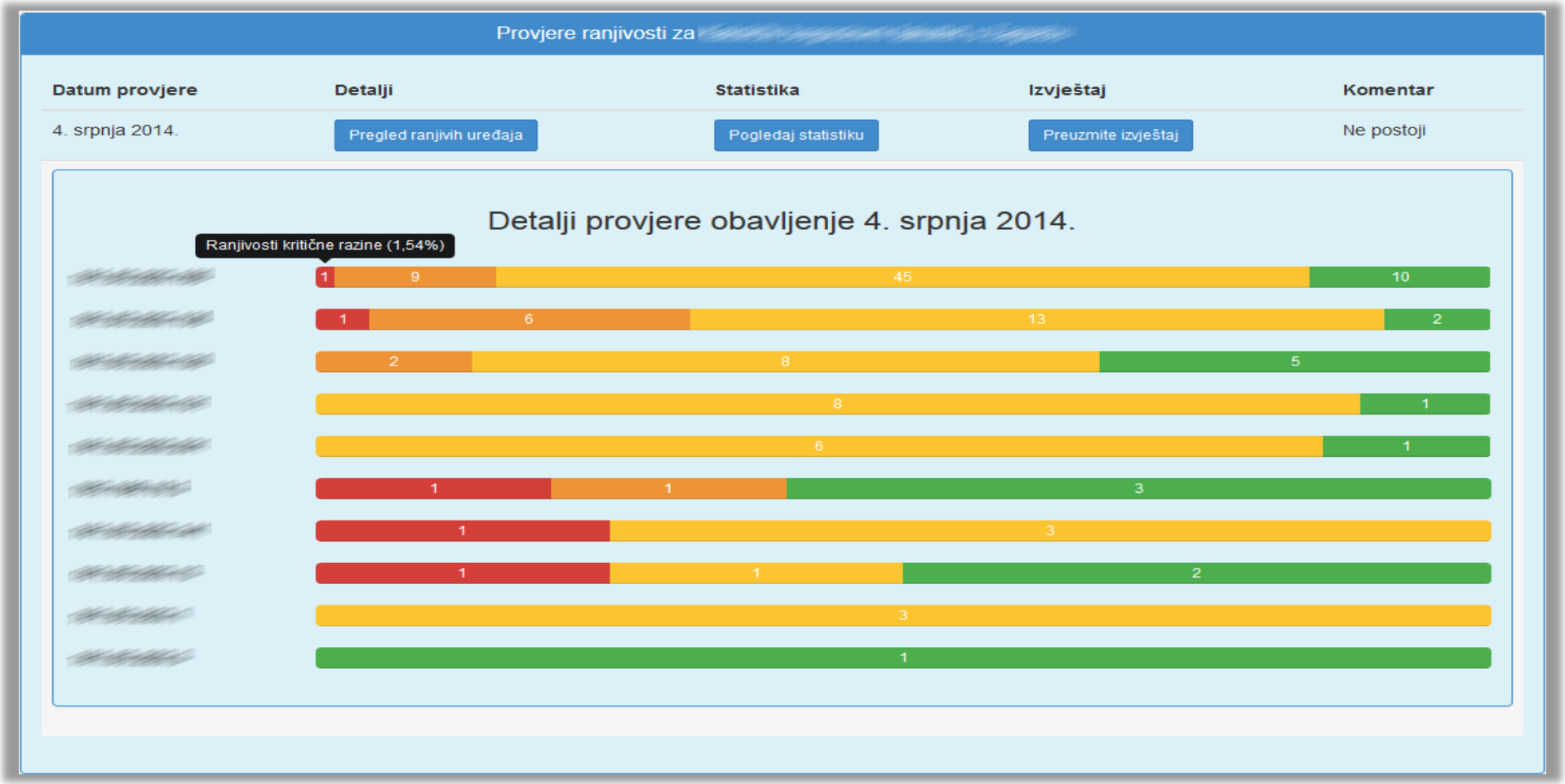
SPORt – izgled sučelja



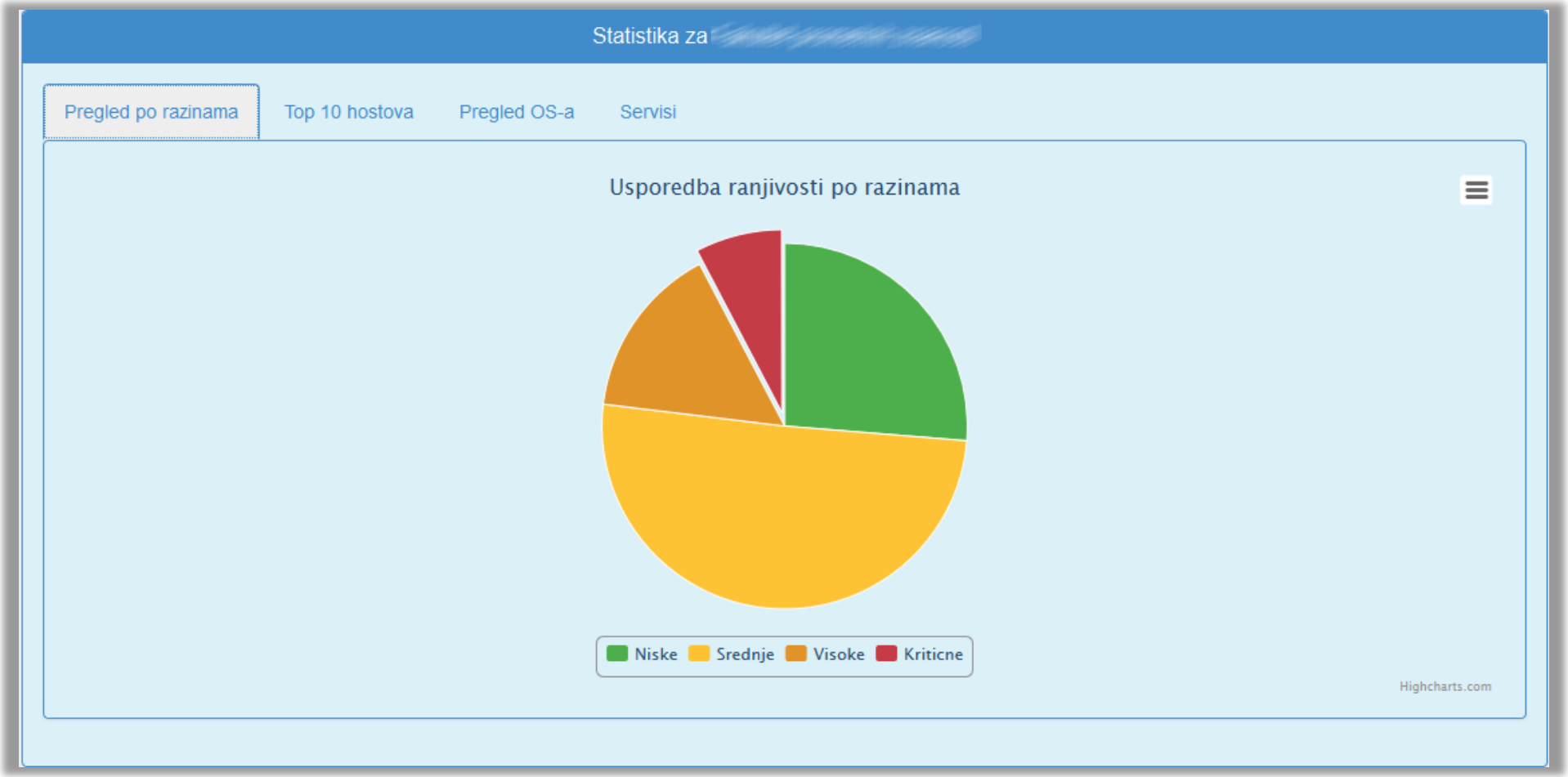
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

SPORt – izgled sučelja



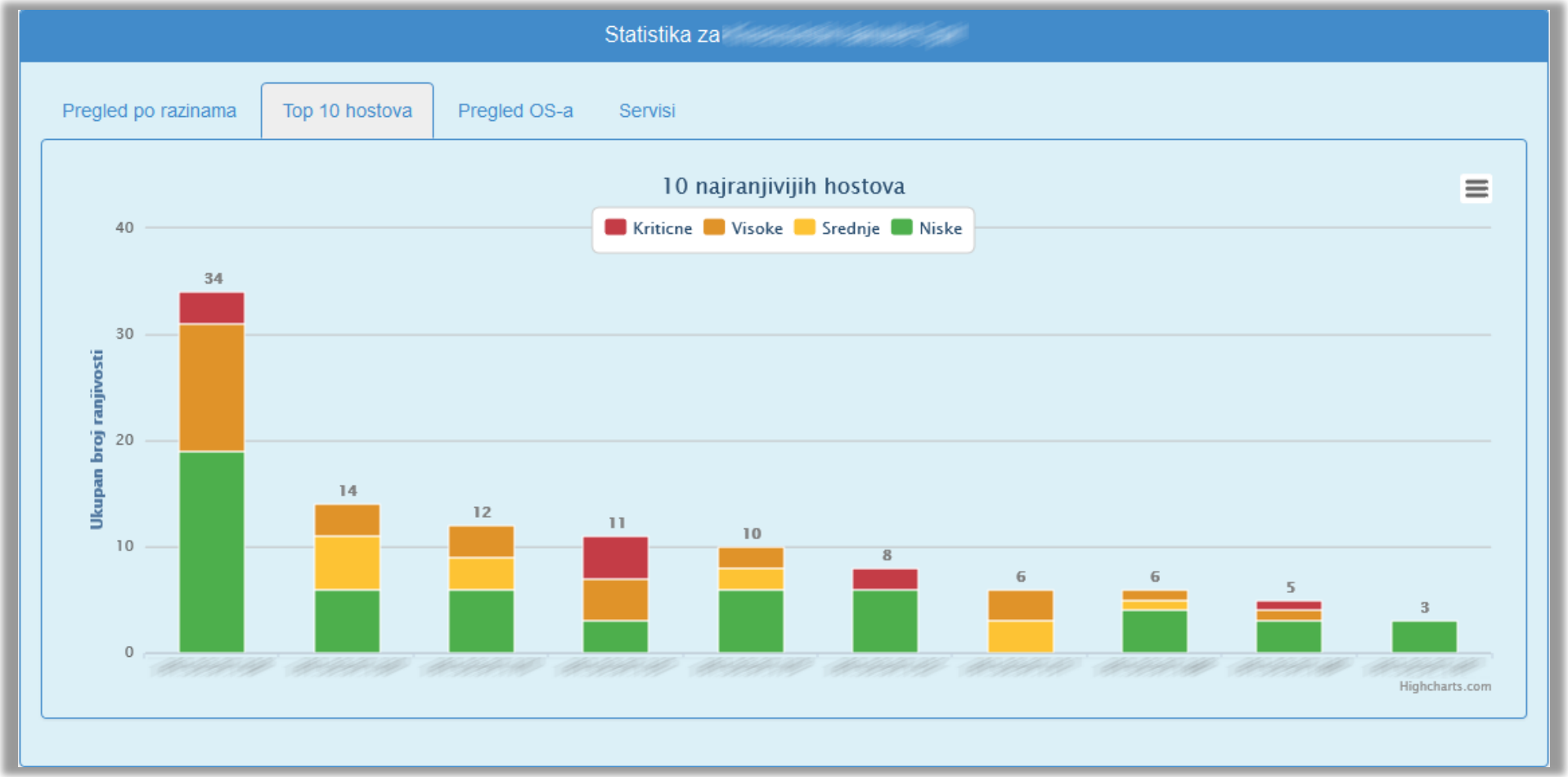
SPORt – izgled sučelja



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

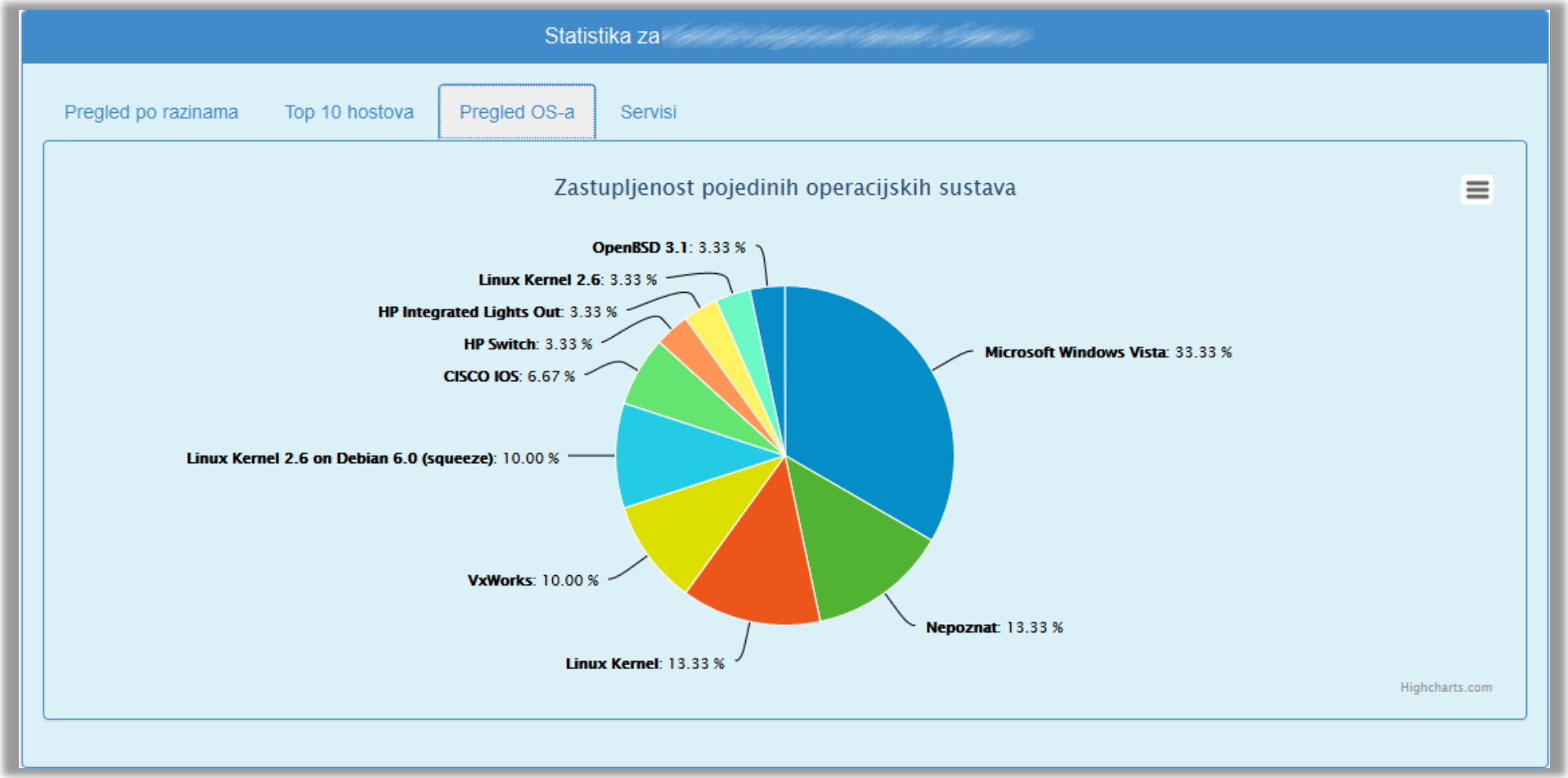
SPORt – izgled sučelja



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

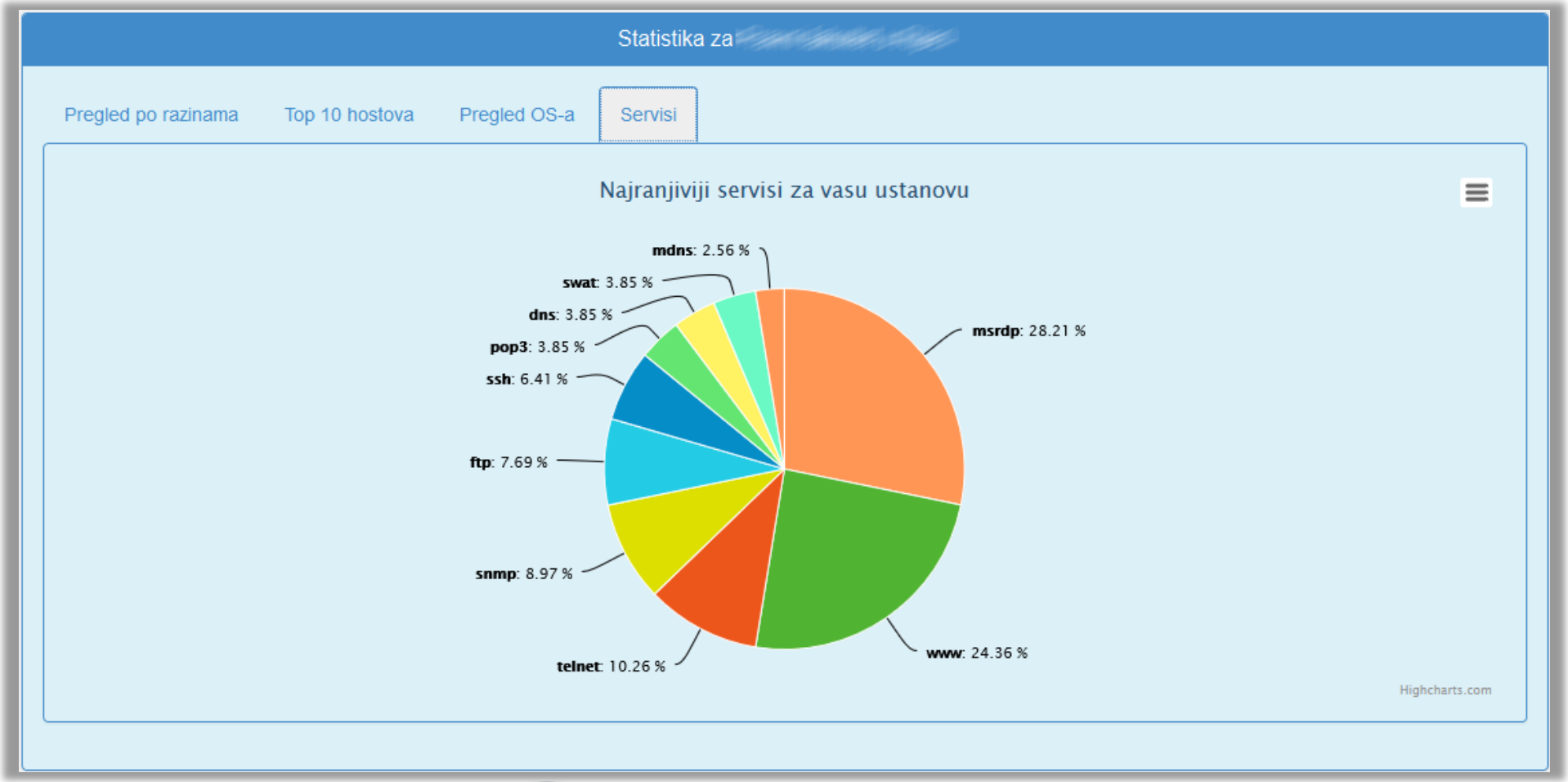
SPORt – izgled sučelja



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

SPORt – izgled sučelja



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Hvala na pažnji!

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT