

Istek AAI identiteta



Nedavno sam rješavao neobičan slučaj korisnika koji se spaja na Internet od kuće preko meže kablovskog operatera. Korisnik je sklopio ugovor s Bnetom i podesio kućni router da pri spajanju obavi autentikaciju koristeći elektronički identitet koji je dobio na ustanovi.

Korisnik se požalio da mu je iznenada uskraćena usluga, a da nije ništa mijenjao u konfiguraciji routera. Pri pokušaju spajanja dobije poruku: **PPTP server not found on specified address**. Zvao je Bnetovu podršku, gdje mu je rečeno da će oni proučiti problem i da će ga netko nazvati. Dani su prolazili, nitko nije zvao. Nazvao je ponovo Bnet, ovog puta je operater bio neljubazan, drsko je odgovorio da je kod njih sve u redu i neka se izvoli obratiti CARNetu. Čak je tvrdio kako on vidi da je router dobio IP adresu, što nije bilo točno, vjerojatno je vidio adresu dodijeljenu modemu.

Korisniku sam sugerirao da se pokuša ulogirati na web sučelju LDAP servisa na ustanovi, kako bi provjerio da li su mu ispravni korisničko ime i zaporka. Sve je prošlo kako treba, a isto korisničko ime i zaporka ispravno su uneseni u konfiguraciju kućnog routera. Dakle problem je u nečem drugom.

U logovima koje radius zapisuje na Linux serveru ustanove pronađeni su brojni zapisi koji pokazuju da korisnikov router svake sekunde obavlja autentikaciju:

```
Sat Nov 5 11:33:50 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:51 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:52 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:53 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:54 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
```

Dakle autentikacija je uspjela, ali zašto router ne dobije IP adresu iz CARNetova adresnog prostora, nego uzaludno pokušava ponovo?

Zatražio sam pomoć AAI@Edu.Hr tima sa Srca. Njihova sugestija uputila me u pravom smjeru. Pružatelji usluga mogu osim korisničkog imena i zaporke provjeravati i neke druge attribute iz LDAP imenika, na primjer datum isteka elektroničkog identiteta! I zaista, korisnik je i dalje imao otvoren račun, ali je u polje **Datum isteka temeljne povezanosti** bio upisan datum koji je već prošao! Korisnik nije student, pa nije dobio račun na godinu dana, dok ne upiše slijedeću godinu. LDAP administrator upisao je proizvoljan datum, koji je u vrijeme otvaranja računa izgledao daleko u budućnosti, ali vrijeme nemilosrdno teče pa je daleka budućnost neprimjetno postala prošlost.

U polje **Datum isteka temeljne povezanosti** moguće je za djelatnike u stalnom radnom odnosu upisati vrijednost **NONE**, obavezno velikim slovima. LDAP administrator će si na taj način olakšati posao, jer neće morati provjeravati kojim je korisnicima isteklo važenje elektroničkog identiteta.

Na kraju, nazvali smo Bnetovu korisničku podršku i objasnili da uzrok problema može biti istek važenja elektroničkog identiteta, tako da ubuduće mogu CARNetove korisnike uputiti da u svojoj ustanovi provjere taj podatak. Ovog je puta operater bio vrlo ljubazan i zahvalio na korisnoj informaciji. Problem riješen.

- [Logirajte](#) [1] se za dodavanje komentara

pet, 2011-12-09 09:48 - Aco Dmitrović **Kategorije:** [Servisi](#) [2]

Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: <https://sysportal.carnet.hr/node/898>

Links

[1] <https://sysportal.carnet.hr/sysportallogin>

[2] <https://sysportal.carnet.hr/taxonomy/term/28>