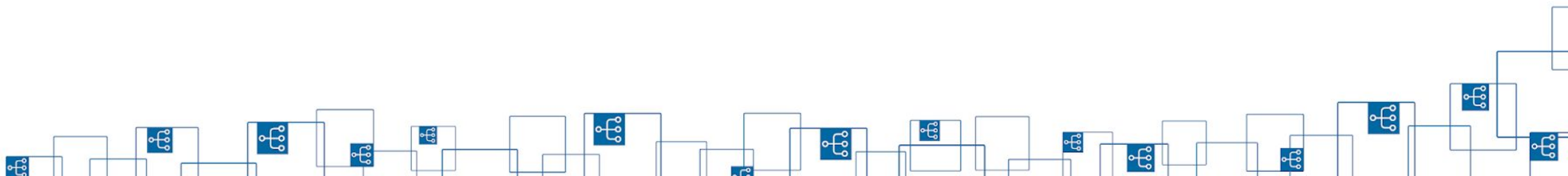


RPZ zóny

Jiří Menšík

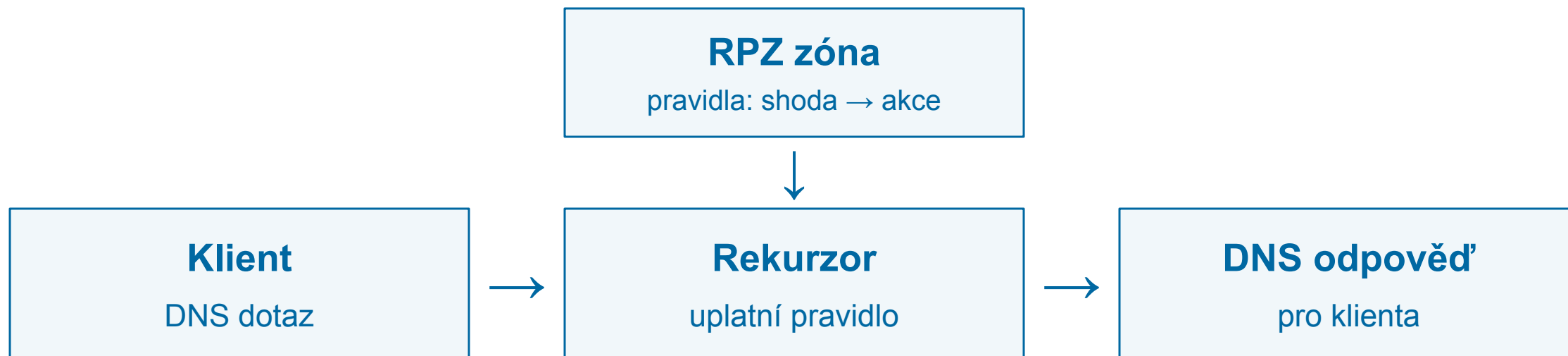
CESNET

Konference e-infrastruktury CESNET 2026 · Praha, 1. října 2026



Co je RPZ zóna?

Response Policy Zone: DNS zóna s pravidly pro úpravu odpovědí rekurzoru.



Pravidla lze sdílet přenosem zóny (AXFR/IXFR).

DNSSEC: přepsaná data nelze ověřit podpisem původní zóny.



Co pravidlo vybírá a co udělá

Podle čeho vybíráme

QNAME: dotazované jméno

Response-IP: IP v odpovědi

NSIP: IP nameserveru

NSDNAME: jméno nameserveru

Jakou akci provedeme

CNAME . (NXDOMAIN)

CNAME *. (NODATA)

CNAME rpz-drop. (DROP: bez odpovědi)

A / AAAA / CNAME
(Local Data: vlastní odpověď)

```
rt.com  IN CNAME  *.poker.cesnet.cz.
```

Pár dat z historie RPZ



Co se změnilo díky ČTÚ

Jednotný strojově čitelný seznam

Dříve

Seznamy MFČR, SÚKL,
SZPI a ÚSKVBL
Ruční přenášení změn

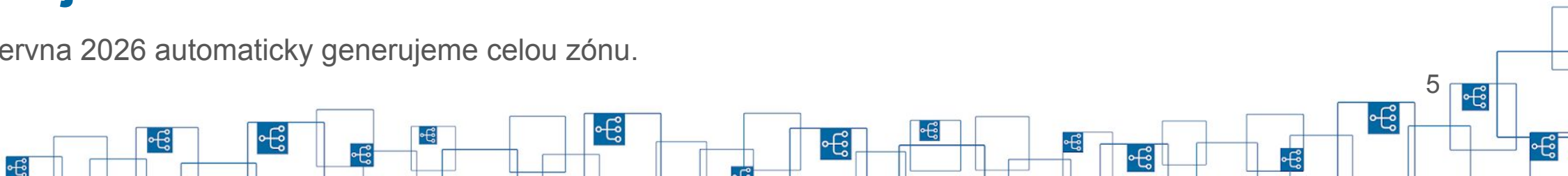


Dnes

Jednotný seznam ČTÚ
Automatické generování zóny

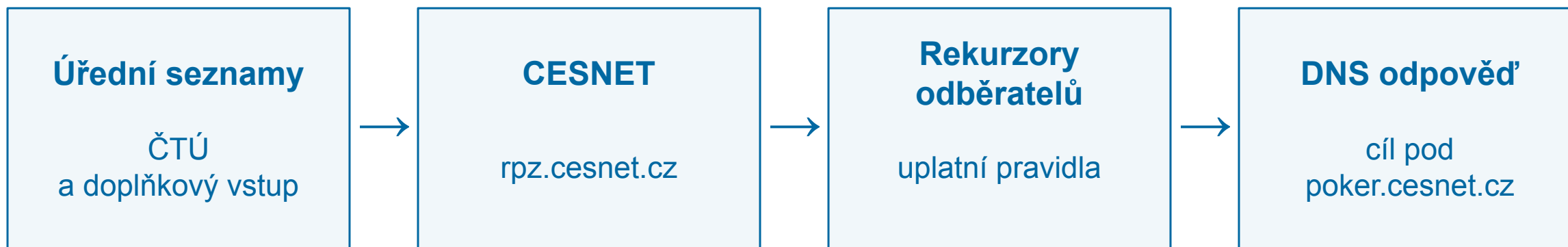
Děkujeme ČTÚ

Od června 2026 automaticky generujeme celou zónu.



Naše použití: veřejná RPZ zóna

rpz.cesnet.cz pro zákonné blokace



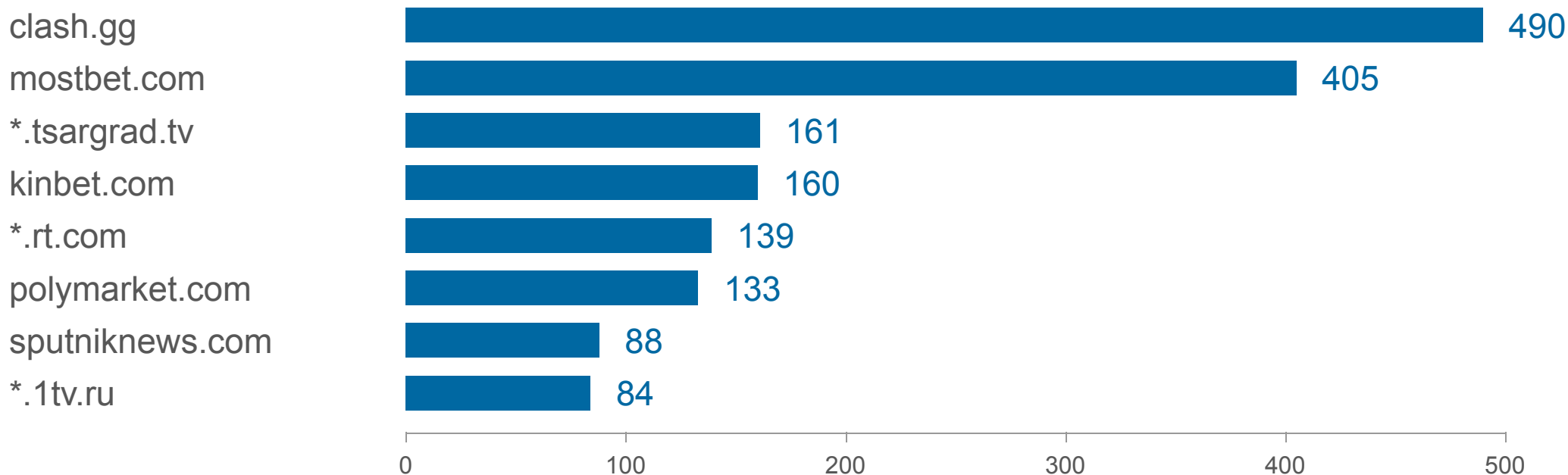
blokovane.internetovehazardnihry.cz CNAME *.poker.cesnet.cz.

Cíl: blokovane.internetovehazardnihry.cz.poker.cesnet.cz.

Nejčastější cíle DNS přesměrování

29. 9. 17:02 – 30. 9. 10:00 CEST (2026)

Celkem 3 031 přiřazených dotazů / 200 pravidel



Jen nsa.cesnet.cz, po průchodu cache. Dotazy, nikoli lidé či všechny blokace.

8 nejčastějších pravidel; dalších 1 036 dotazů bez přiřazení je mimo graf.

Co může vidět blokovací web

Modelový požadavek s vymyšlenými údaji

URL: `http://blokovany-web.example/hledat?q=ukazka`

GET `/hledat?q=ukazka` HTTP/1.1

Host: `blokovany-web.example`

Referer: `http://odkaz.example/clanek`

User-Agent: `UkazkovyProhlizec/1.0`

cesta a parametry

původní doména

hlavičky, pokud je
klient pošle

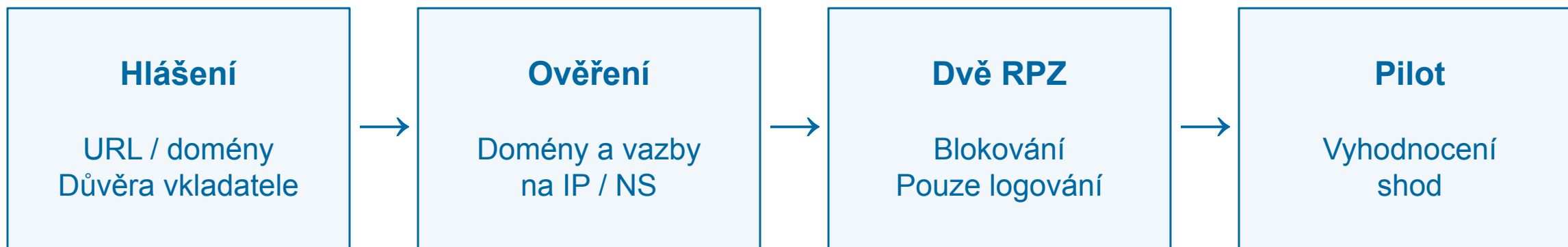
Web navíc vidí zdrojovou IP spojení.

Při DNS přesměrování zůstává původní URL.

HTTPS: odmítnutí certifikátu obvykle zabrání HTTP požadavku i access logu.
DNS blokace přitom může fungovat.

Další využití: ochrana před phishingem

Zvažované využití komunitních hlášení phishingu



Ověřené domény blokovat; související IP / NS nejdřív měřit.

Shodná IP či NS může patřit i legitimním doménám.