



NETTLES CONSULTING

Ochrana před framing útoky včera a dnes

Jan Kopriva

Security Consultant & Trainer

jan.kopriva@nettles.cz

„Framing“ útoky

- Schopnost zobrazit cizí webový obsah na vlastní doméně může být velmi dobře legitimně využitelná
- Problémem je, že je i snadno zneužitelná s pomocí iframe
 - Legitimní stránky organizace nahrané do pozadí „pod“ falešné přihlašovací okno
 - Legitimní přihlašovací okno „překryté“ falešným přihlašovacím oknem
 - ...
- Škodliví aktéři v praxi výše uvedené mechanismy rádi využívají
 - Značné procento „generických“ phishingových stránek zobrazuje falešný přihlašovací formulář k e-mailu či jiné službě nad webovými stránkami běžícími na doméně příjemce souvisejícího phishingového e-mailu

Firefox Can't O

To protect your security,
To see this page, you ne

[Learn more...](#)

☐ Report errors like thi



honza@google.com

Password

☐ Remember me

Continue

site has embedded it.

ite in New Window

Jak se lze nežádoucímu „framingu“ vlastních stránek bránit?

- K dispozici máme 2 technologické mechanismy založené na doplňkových HTTP hlavičkách, které mohou nechtěnému „framingu“ zabránit
 - X-Frame-Options
 - Content Security Policy s direktivou frame-ancestors



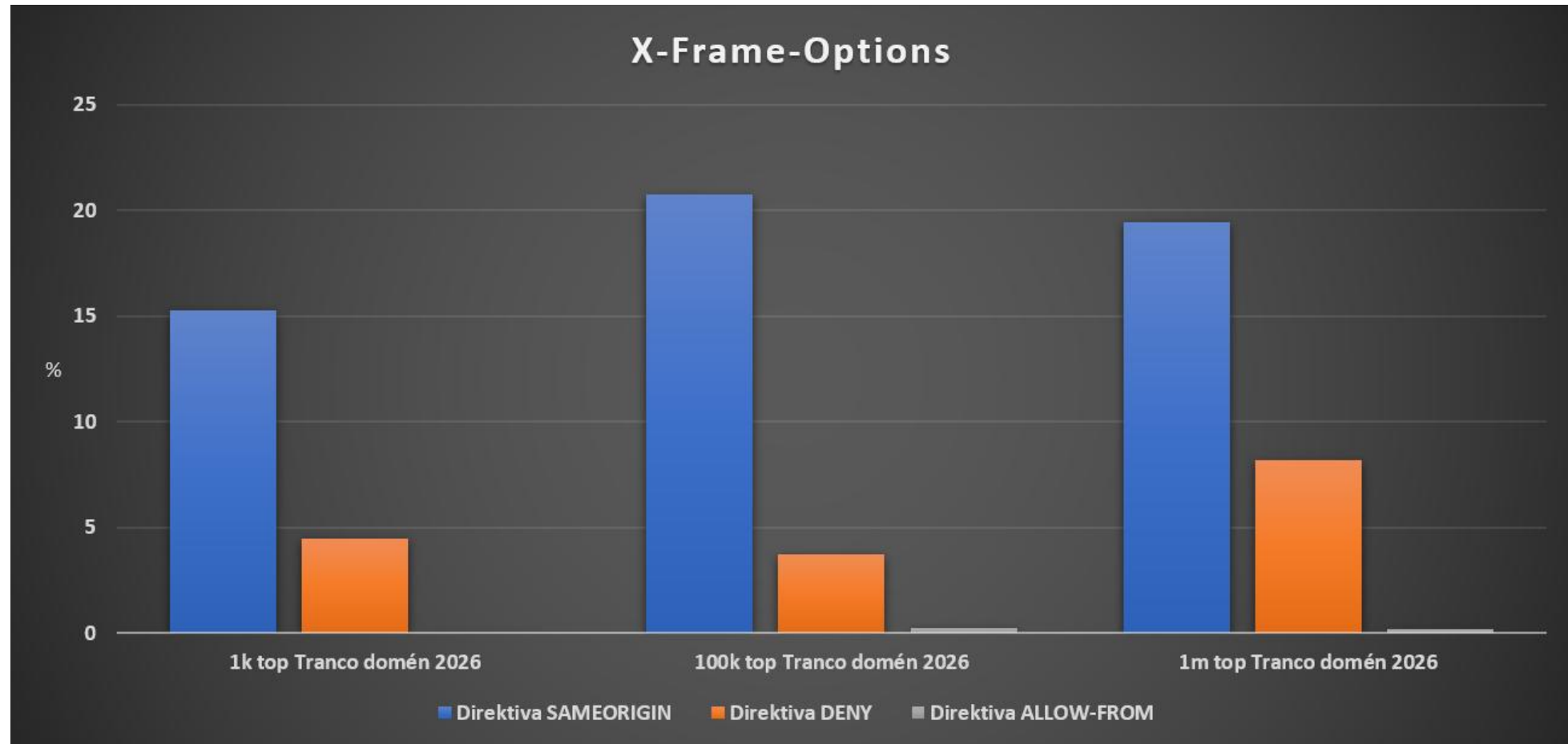
X-Frame-Options

- Historická, byť stále podporovaná hlavička
- Podporuje pouze relativně jednoduché nastavení povoleného framingu
 - DENY – framing plošně zakázán
 - SAMEORIGIN – framing povolen na stránkách ze stejného zdroje/domény
 - ALLOW-FROM – framing povolen ze specifických zdrojů/domén
- Možné používat paralelně s modernějším CSP jako „fallback“ pro starší prohlížeče (je-li něco takového relevantní)

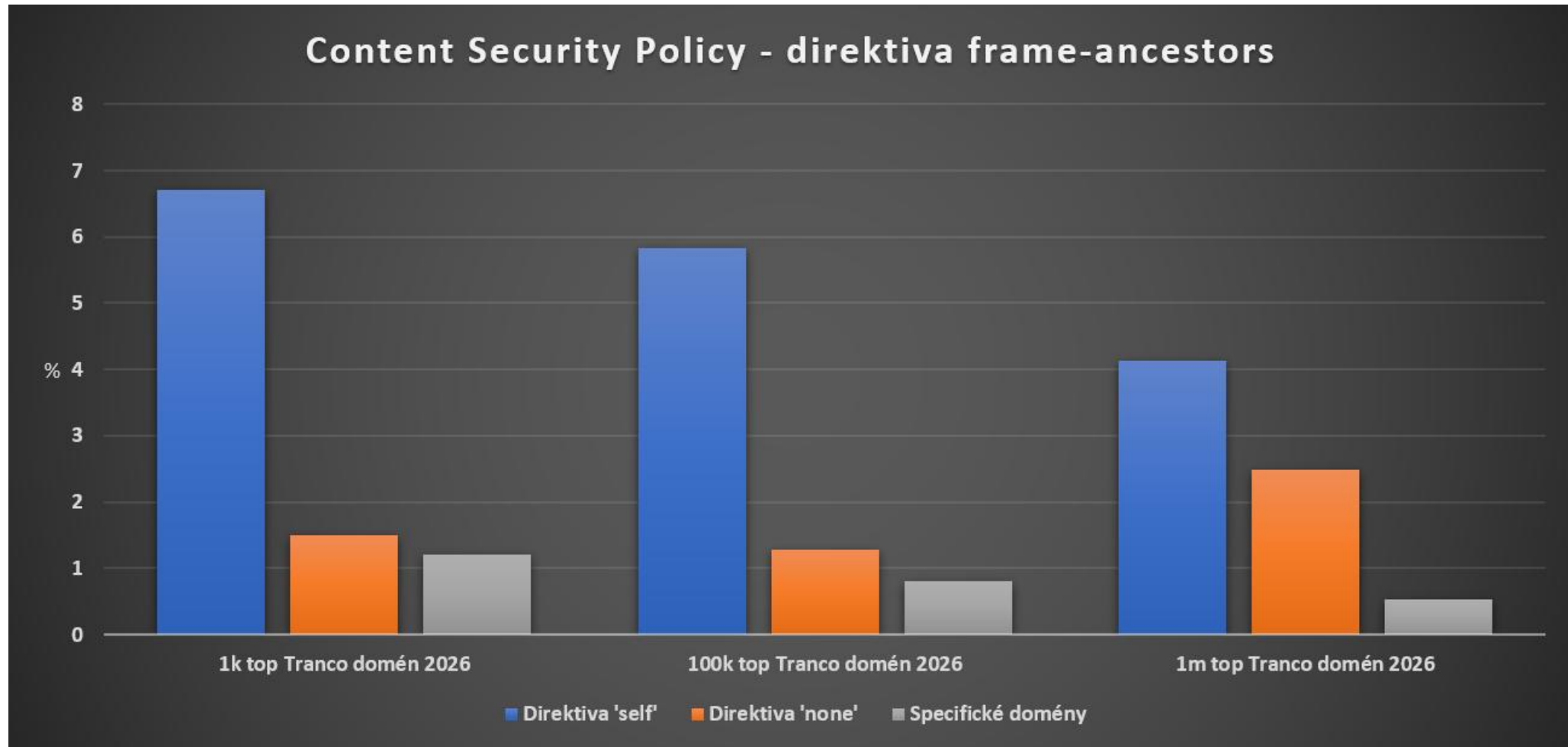
Content Security Policy

- Bezpečnostní hlavička umožňující provést komplexní nastavení „bezpečnostní politiky“ pro určitou doménu
- Její direktiva „frame-ancestors“ umožňuje provádět o něco širší nastavení framingu než X-Frame-Headers
 - Obdobné parametry jako XFH ('none' ~ DENY, 'self' ~ SAMEORIGIN, ...)
 - Podpora některých pokročilých nastavení (wildcardy na úrovni subdomén apod.)

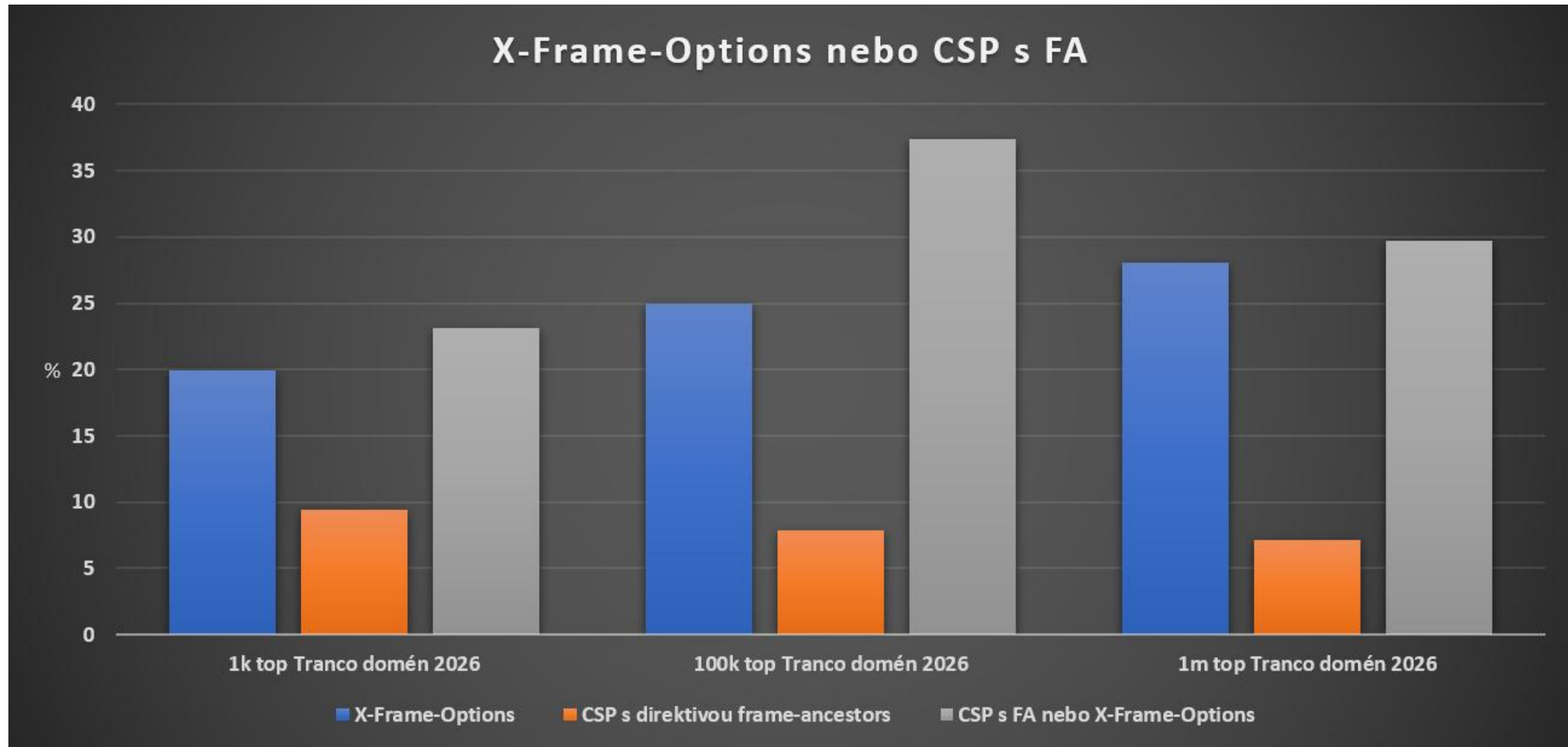
Praktické využívání „framing“ hlaviček – svět



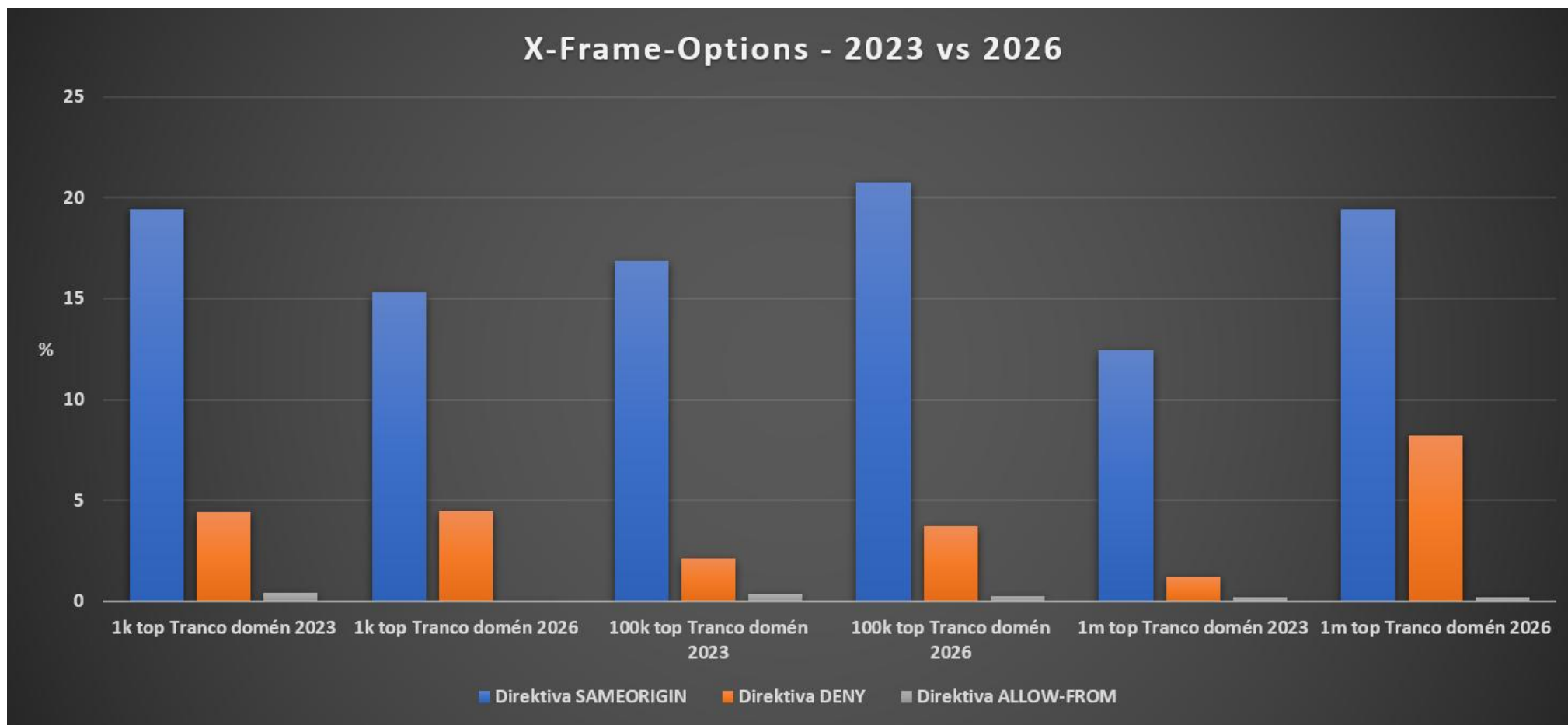
Praktické využívání „framing“ hlaviček – svět



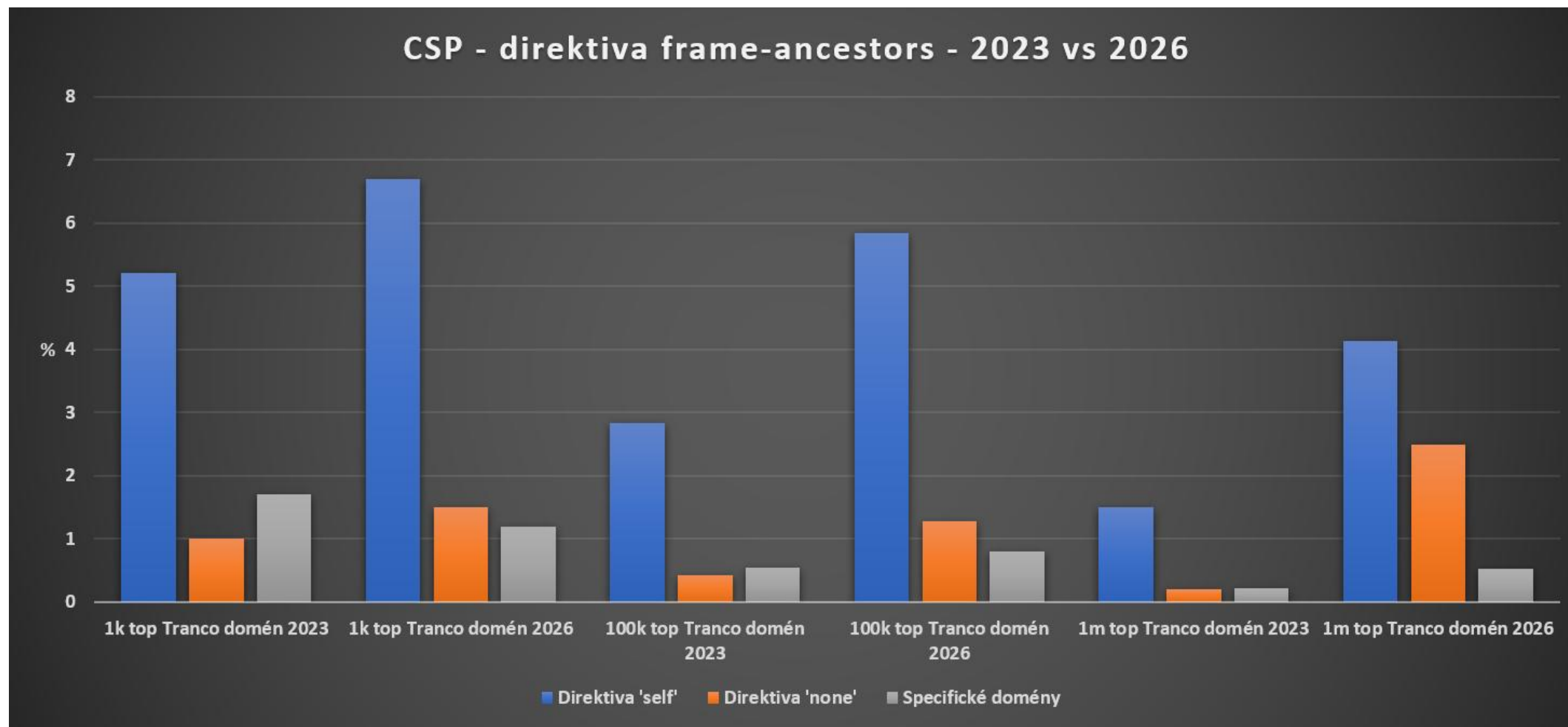
Praktické využívání „framing“ hlaviček – svět



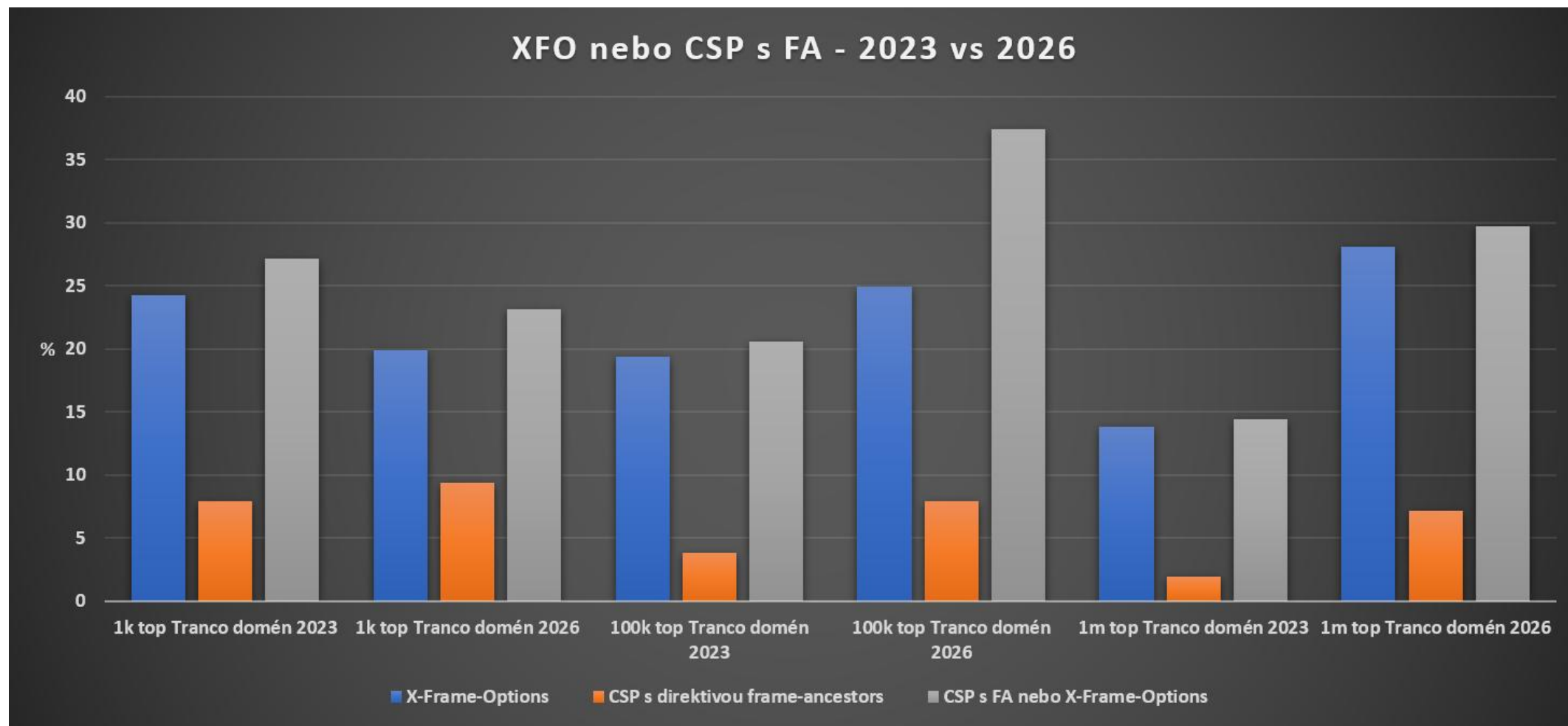
Změna za poslední 3 roky



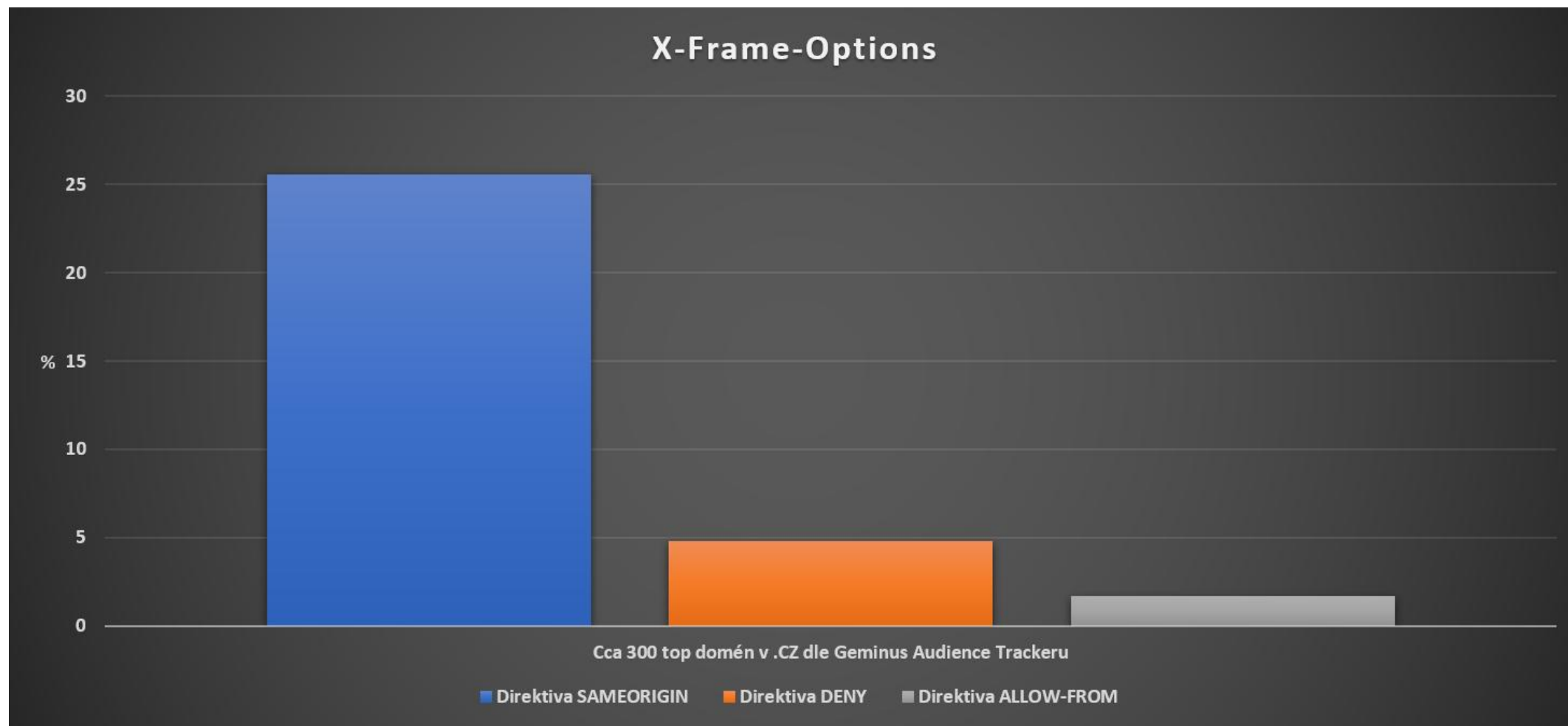
Změna za poslední 3 roky



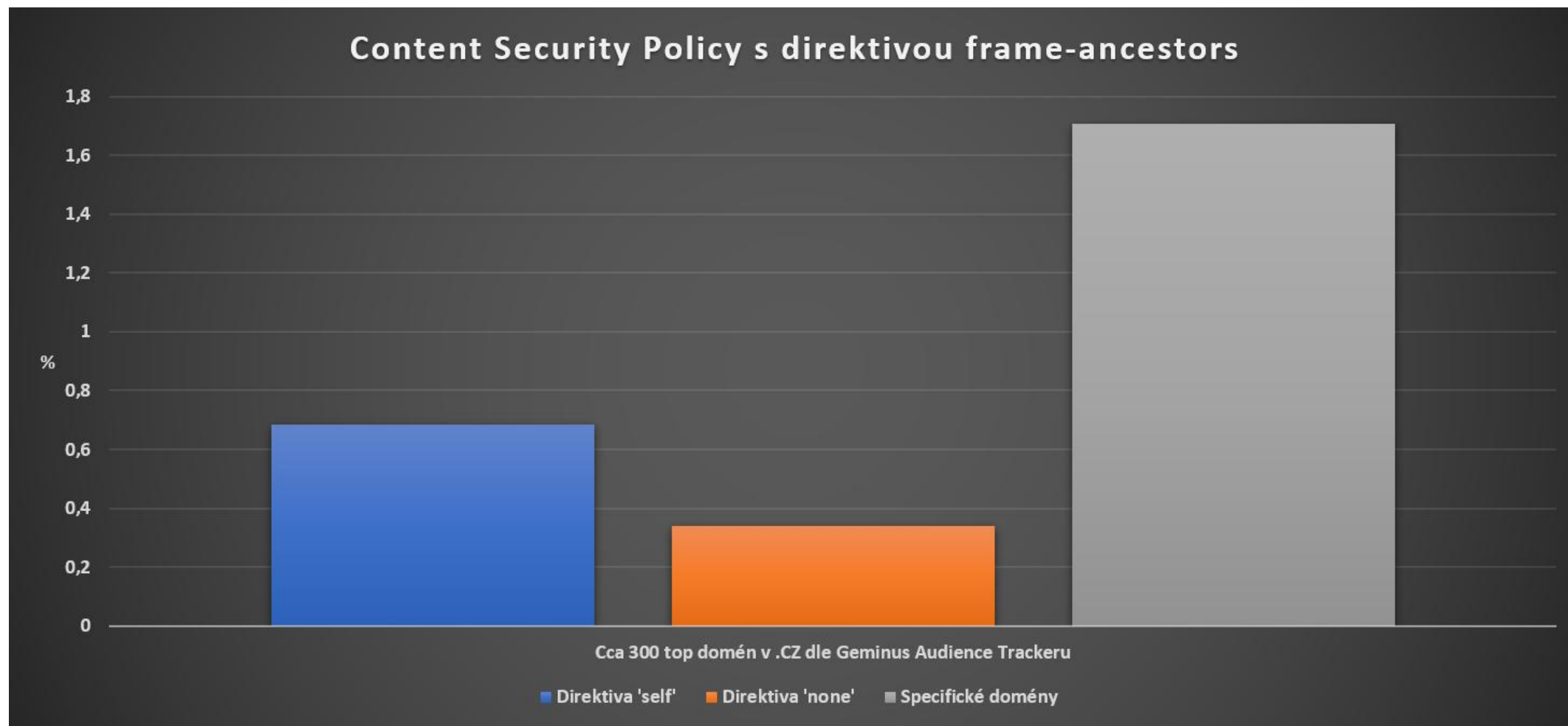
Změna za poslední 3 roky



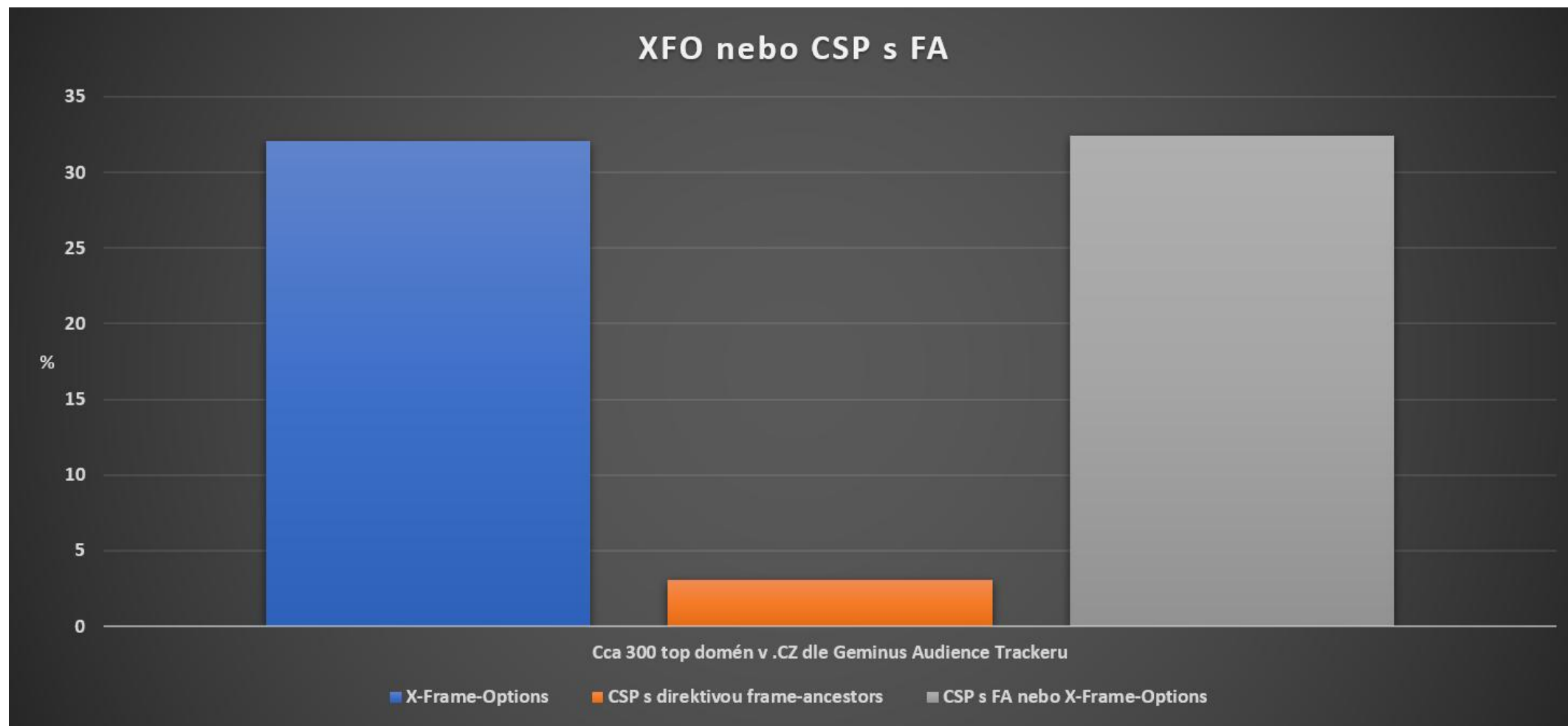
Praktické využívání „framing“ hlaviček – ČR



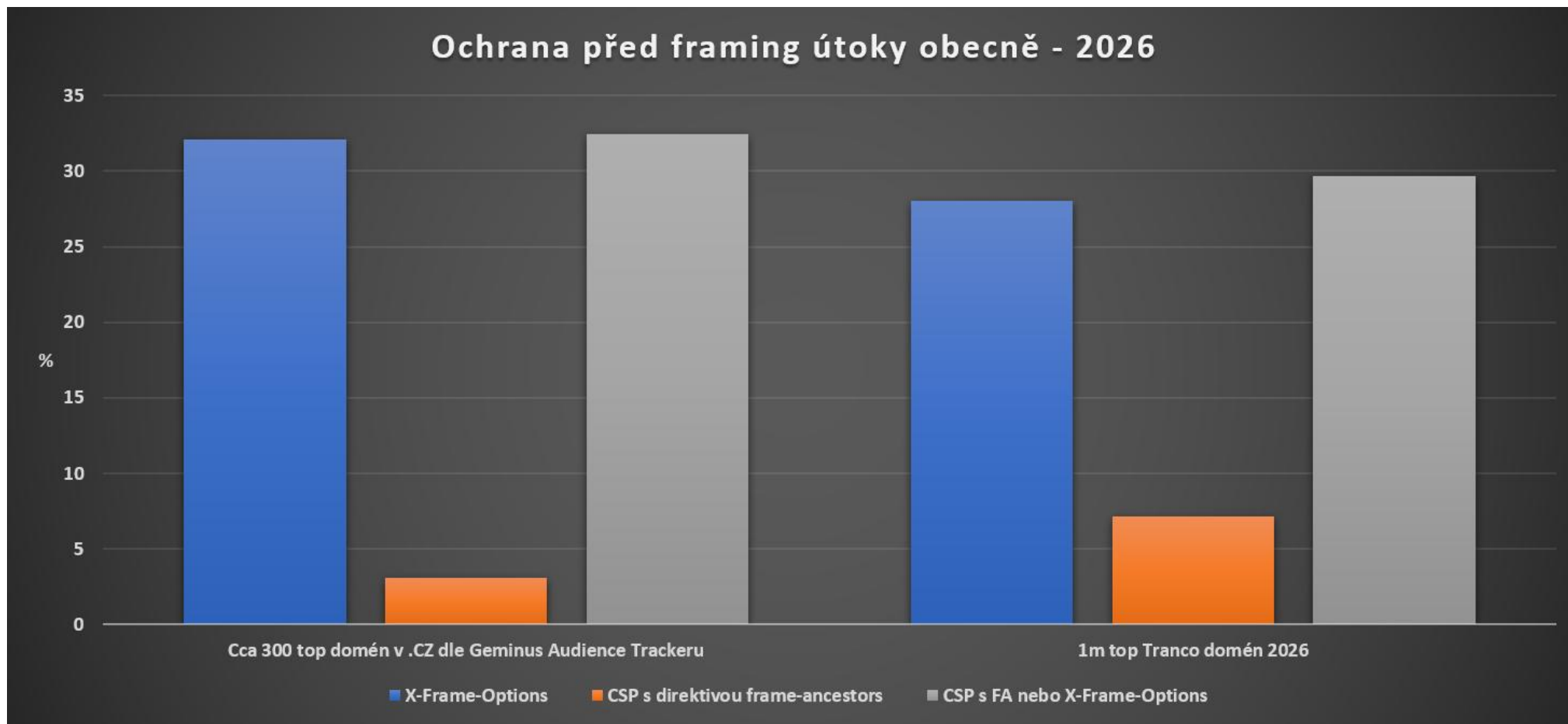
Praktické využívání „framing“ hlaviček – ČR



Praktické využívání „framing“ hlaviček – ČR



Svět vs. ČR*



Vhodná cesta vpřed? Nastavení CSP (a volitelně i XFO)

- Jak nastavit frame-ancestors direktivu Content Security Policy?
 - Pokud není framing z vaší strany zamýšlený, pak 'none'
 - Pokud je žádoucí umožnit načítat vaší stránku na jiných doménách, uveďte je explicitním výčtem
 - Pokud je žádoucí umožnit načítat vaší stránku na libovolné doméně
 - Vzdělávejte uživatele i zákazníky
 - Není-li to nezbytné, neprovazujte na dané doméně přihlašovací mechanismy ani jiné potenciálně citlivé formulářové funkcionality

Děkuji Vám za pozornost!



NETTLES CONSULTING

Q&A



NETTLES CONSULTING