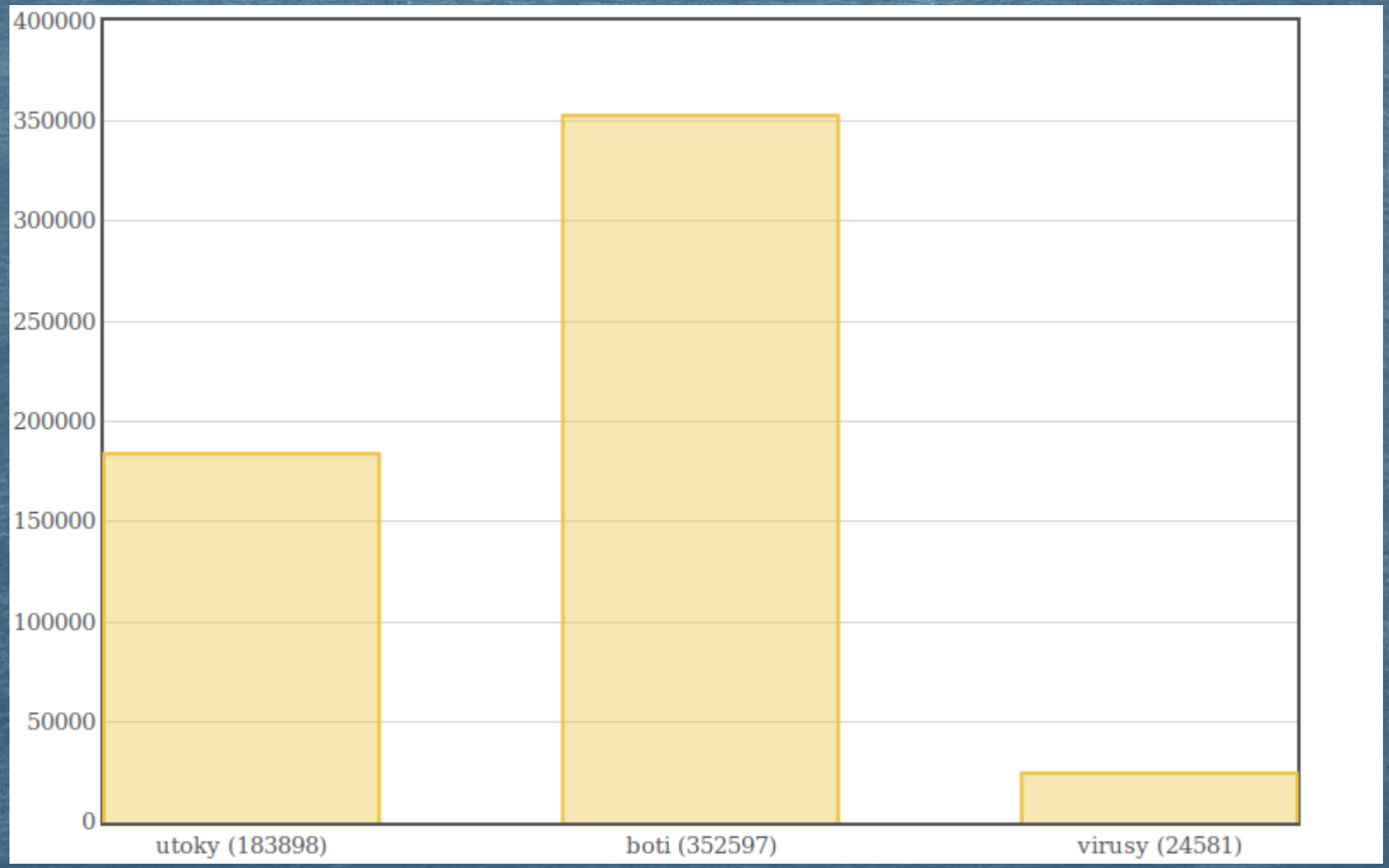
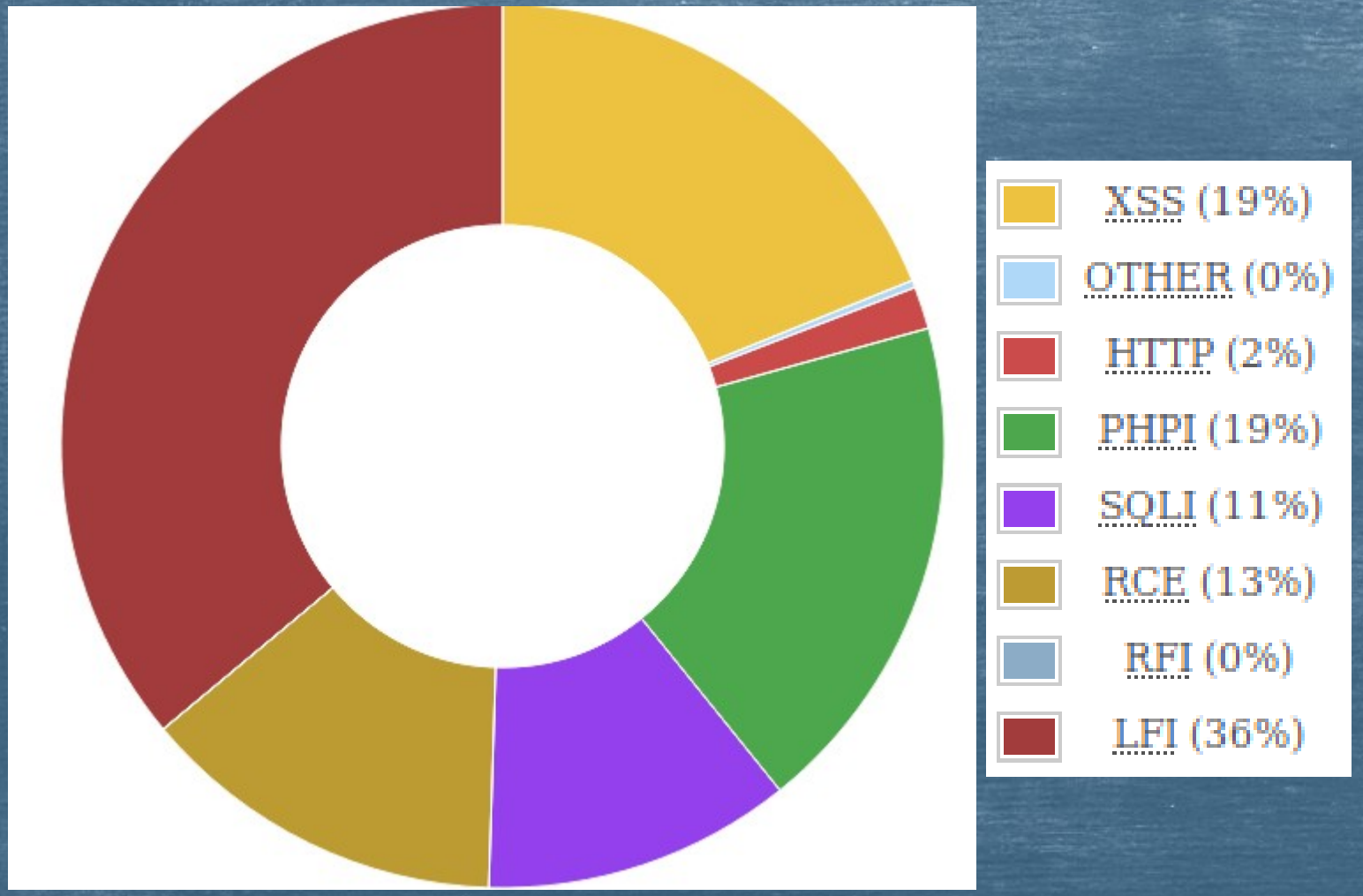
Jozef Sudolský
Jozef.sudolsky@elbia.sk
ELBIA, s. r. o.

Analýza kybernetických útokov na systémy WordPress

O čom bude reč..



Typy útokov



LFI: Local File Inclusion

XSS: Cross Site Scripting

PHPI: PHP Code Injection

RCE: Remote Code Execution

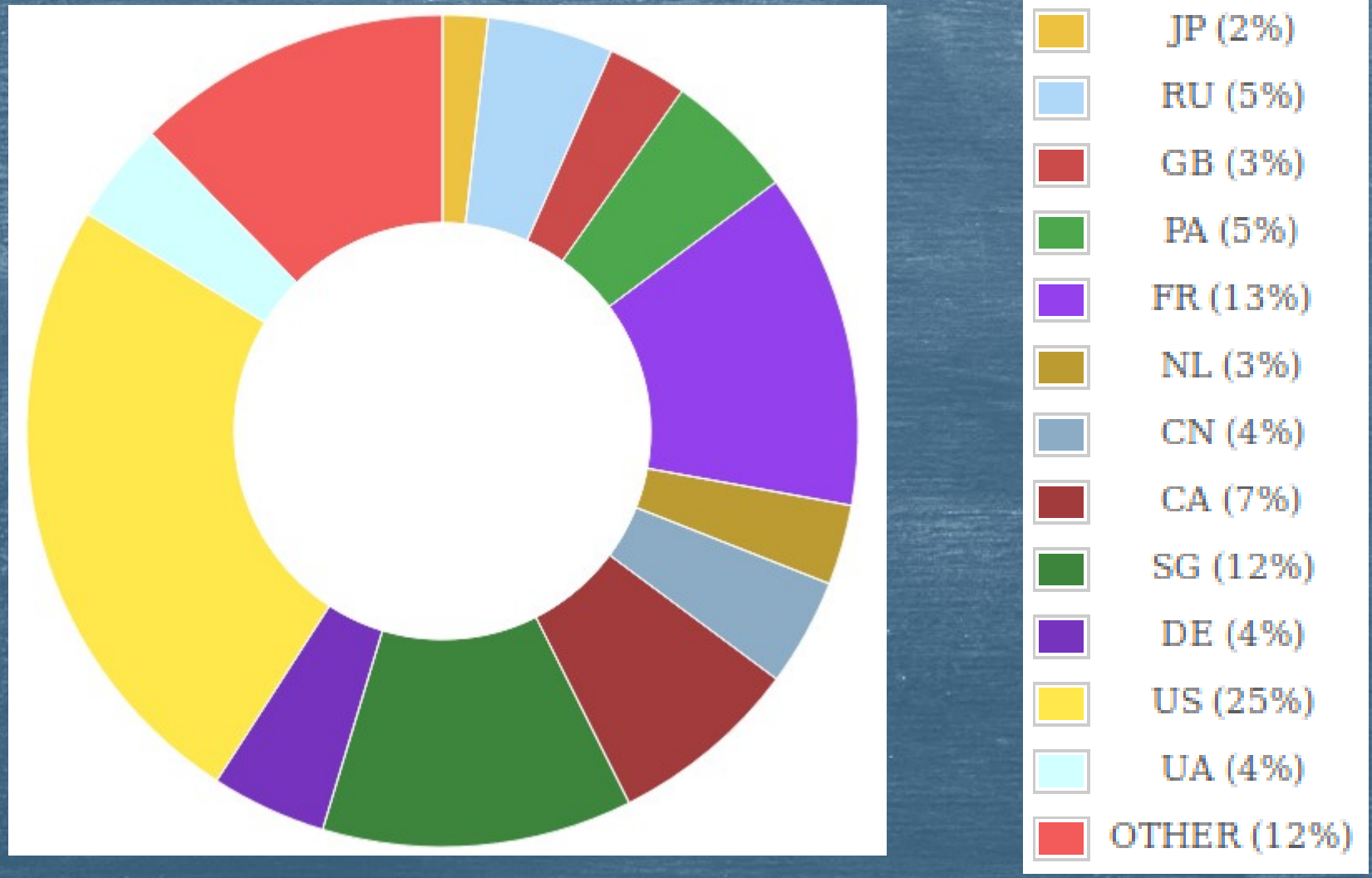
SQLI: SQL Injection

HTTP: HTTP Protocol Violation

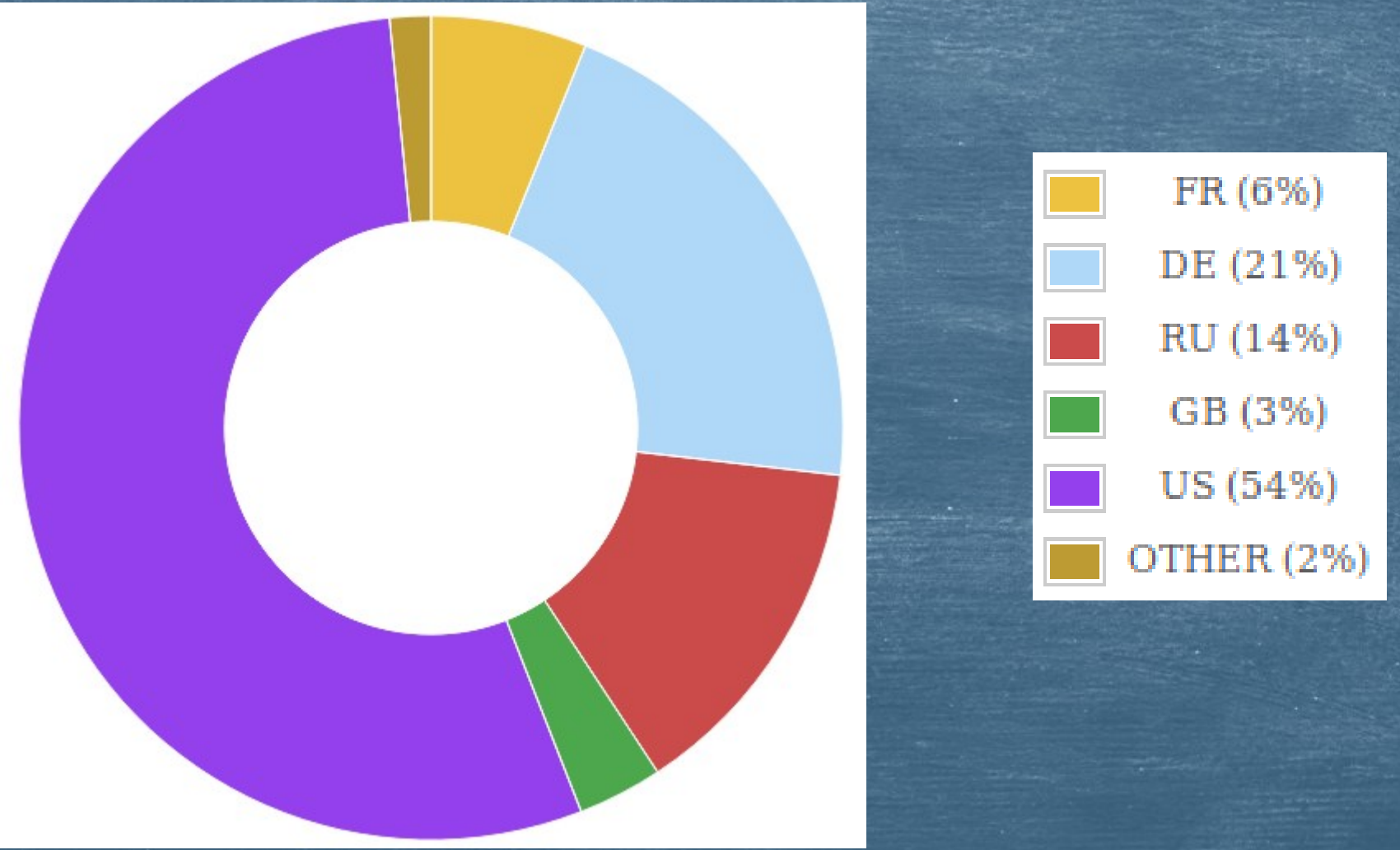
RFI: Remote File Inclusion

OTHER: Iný typ útoku

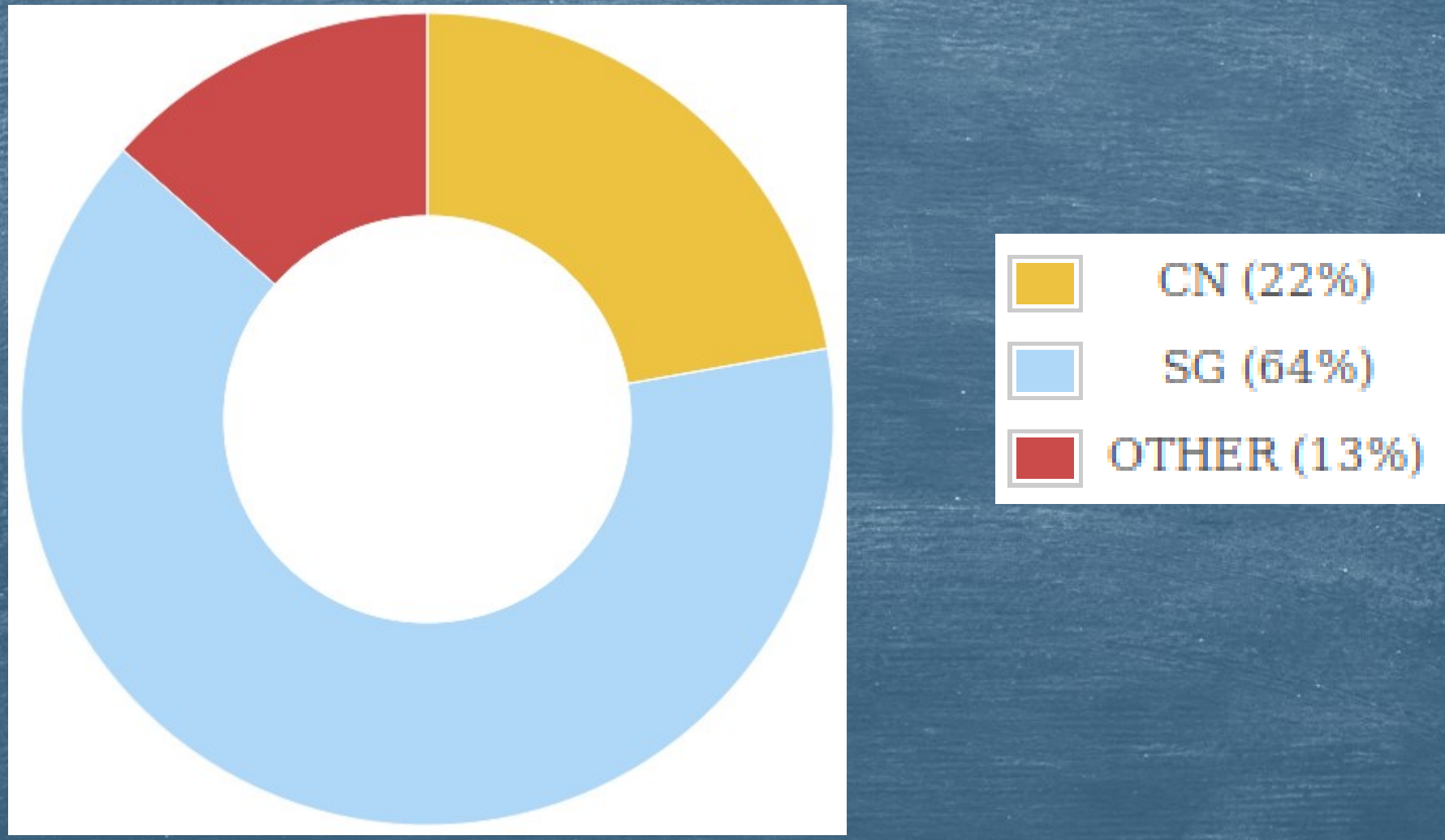
Krajiny pôvodu útokov



Krajiny pôvodu robotov



Krajiny pôvodu vírusov



Prečo je to problém?

- Výpadky (vyčerpanie zdrojov, poškodenie dát, ..)
- Finančné straty
- Únik dát (osobné, obchodné, ..)
- Poškodenie mena

Ako sa brániť

- Vlastný jednoduchý firewall vytvorený na základe prezentovaných dát
- Firewall vo forme pluginu
- Webový aplikačný firewall (WAF) prevádzkovaný poskytovateľom

Vlastný firewall

- Komplikovaná implementácia
- Veľmi nízka náročnosť na serverové zdroje
- Selektívna účinnosť

Vlastný firewall

- 50% útokov pochádza len z 3 krajín (US, FR, SG)
- 89% (zlých) robotov pristupuje len z 3 krajín (US, DE, RU)
- 86% vírusov pochádza len z 2 krajín (SG, CN)
- 74% útokov je 3 typov (LFI, XSS, PHPI)

Vlastný firewall

```
SetEnvIf GEOIP_COUNTRY_CODE US banned
SetEnvIf GEOIP_COUNTRY_CODE FR banned
SetEnvIf GEOIP_COUNTRY_CODE SG banned
SetEnvIf GEOIP_COUNTRY_CODE DE banned
SetEnvIf GEOIP_COUNTRY_CODE RU banned
SetEnvIf GEOIP_COUNTRY_CODE CN banned
SetEnvIf User-Agent "Googlebot" whitelist
Order Deny,Allow
Deny from env=banned
Allow from env=whitelist
```

Firewall vo forme pluginu

- Jednoduchá implementácia
- Vysoká náročnosť na serverové zdroje
- Stredná účinnosť
- Wordfence Security, Jetpack, BulletProof security

Wordfence Security

- CPU: 22 sekúnd procesorového času
- RAM: 206 MB
- Účinnosť: 2 / 51

Jetpack

- CPU: 17 sekúnd procesorového času
- RAM: 143 MB
- Účinnosť: 3 / 51

BulletProof security

- CPU: 9 sekúnd procesorového času
- RAM: 77 MB
- Účinnosť: 30 / 51

Webový aplikačný firewall

- Vrstva nad WordPressom resp. PHP
- Jeden systém pre celý server – lepšia analýza útokov
- Integrácia s antivírusovým softvérom

Webový aplikačný firewall

- O implementáciu sa stará poskytovateľ hostingu
- Nízka náročnosť na serverové zdroje
- Vysoká účinnosť

Webový aplikačný firewall

- CPU: 7 sekúnd procesorového času
- RAM: 51 MB
- Účinnosť: 26 / 51

Webový aplikačný firewall

	RAM	CPU	Účinnosť
Wordfence Security	**206**	**22**	**2 / 51**
Jetpack	143	17	3 / 51
BulletProof security	77	9	**30 / 51**
WAF	**51**	**7**	26 / 51

Priestor pre vaše otázky

Ďakujem za pozornosť!