



Jakým zranitelnostem jsme letos čelili a na jaké je třeba se do budoucna zaměřit

Jan Kopřiva

jan.kopriva@alef.com

 @jk0pr

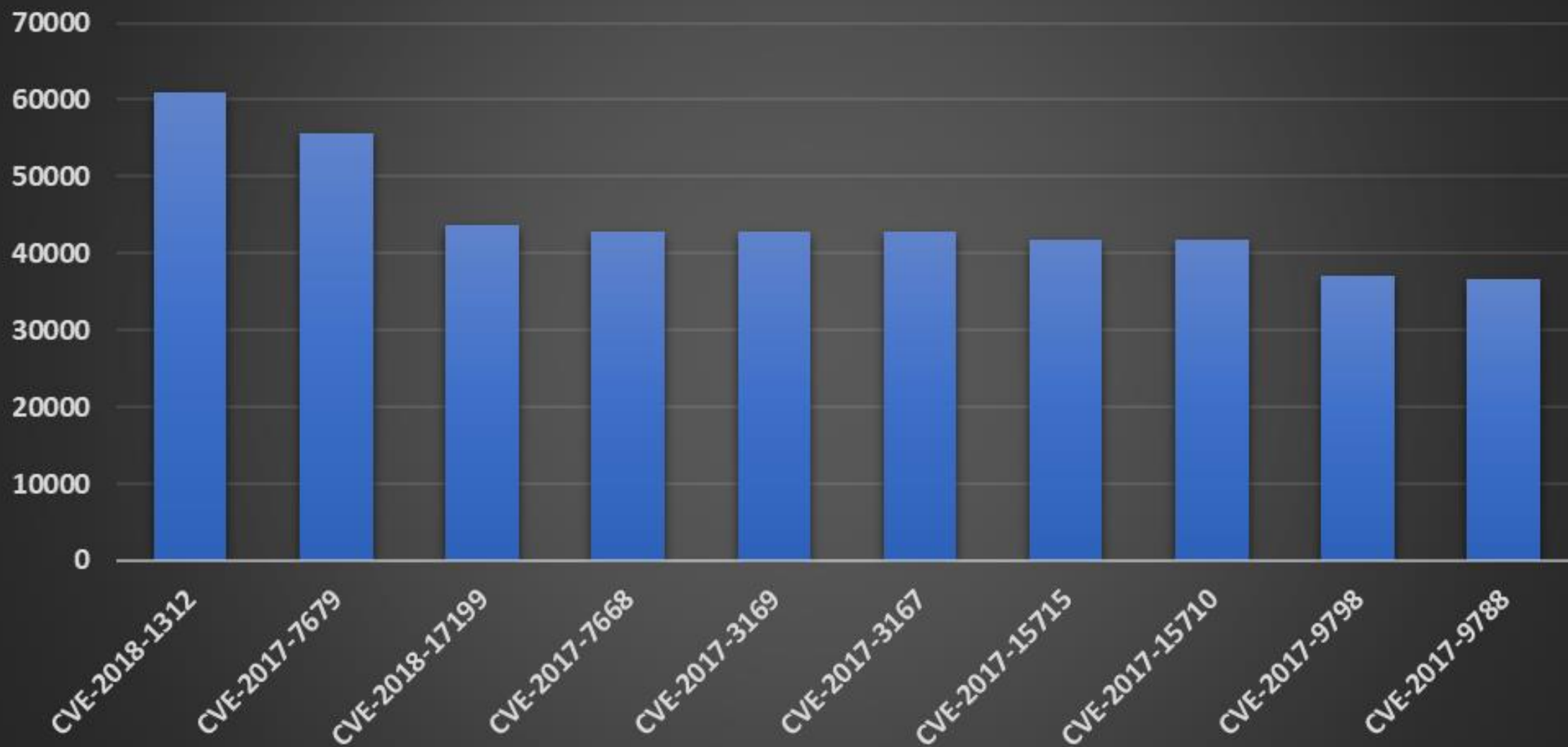
ALEF CSIRT



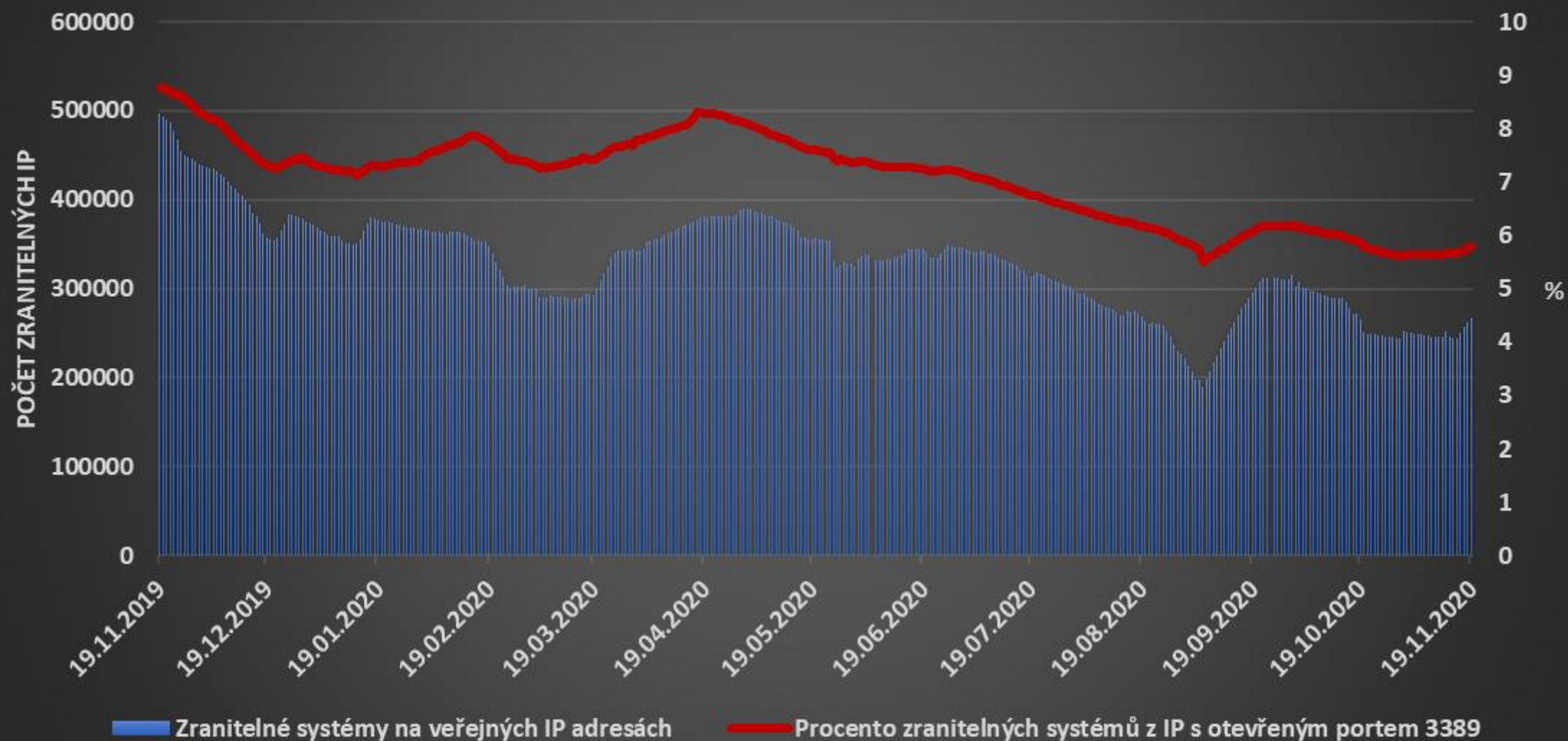
TLP: WHITE

CVE	Počet zranitelných systémů	CVSSv3
<u>CVE-2019-0211</u>	3 357 835	7.8
<u>CVE-2019-12525</u>	1 219 716	9.8
<u>CVE-2015-1635</u>	374 113	N/A, CVSSv2 10.0
<u>CVE-2019-13917</u>	268 409	9.8
<u>CVE-2019-10149</u>	264 655	9.8
<u>CVE-2019-0708</u>	246 869	9.8
<u>CVE-2014-0160</u>	204 878	7.5
<u>CVE-2019-9787</u>	83 951	8.8
<u>CVE-2019-12815</u>	80 434	9.8
<u>CVE-2018-6789</u>	76 344	9.8

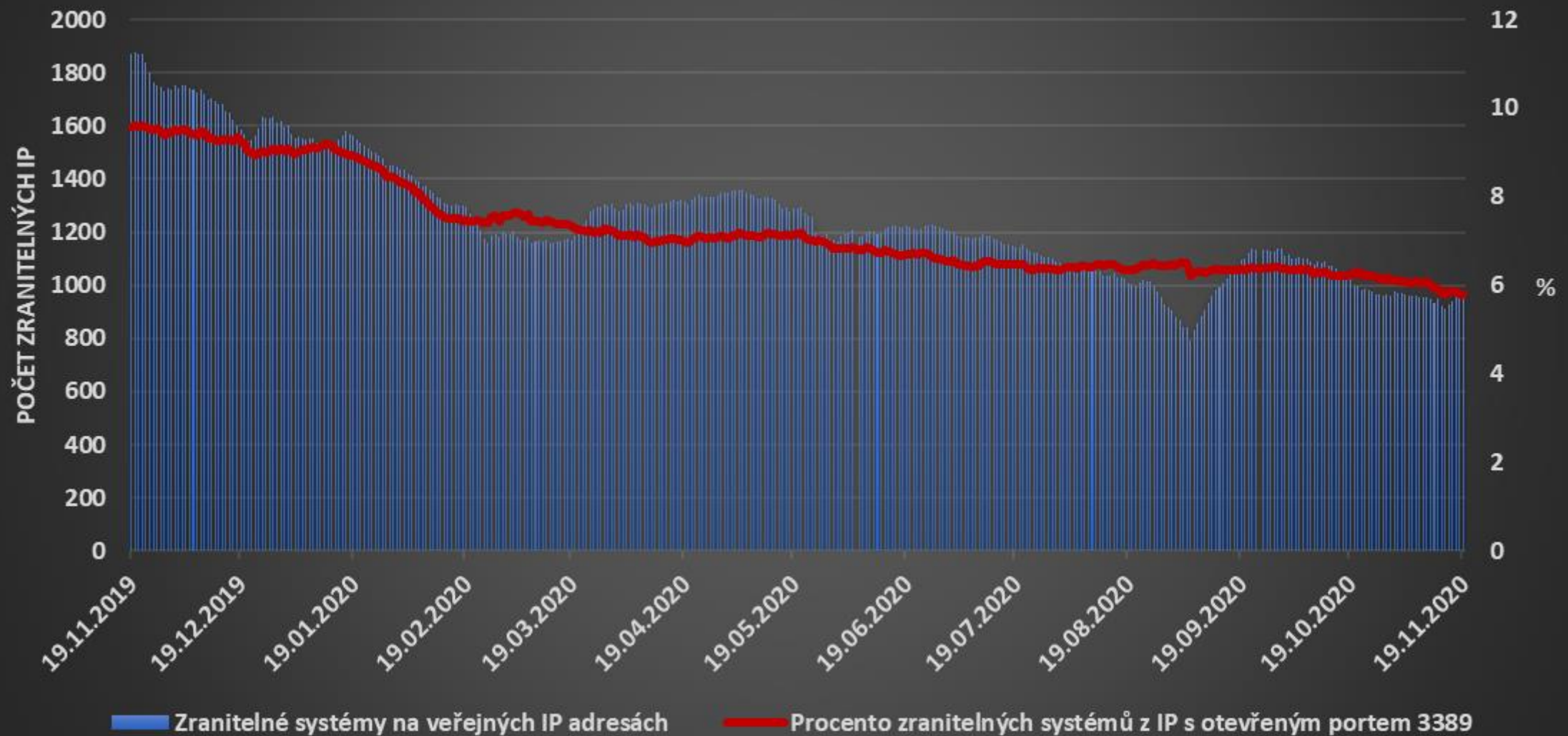
Zranitelnosti na českém internetu - Apache



BlueKeep - Globální detekce



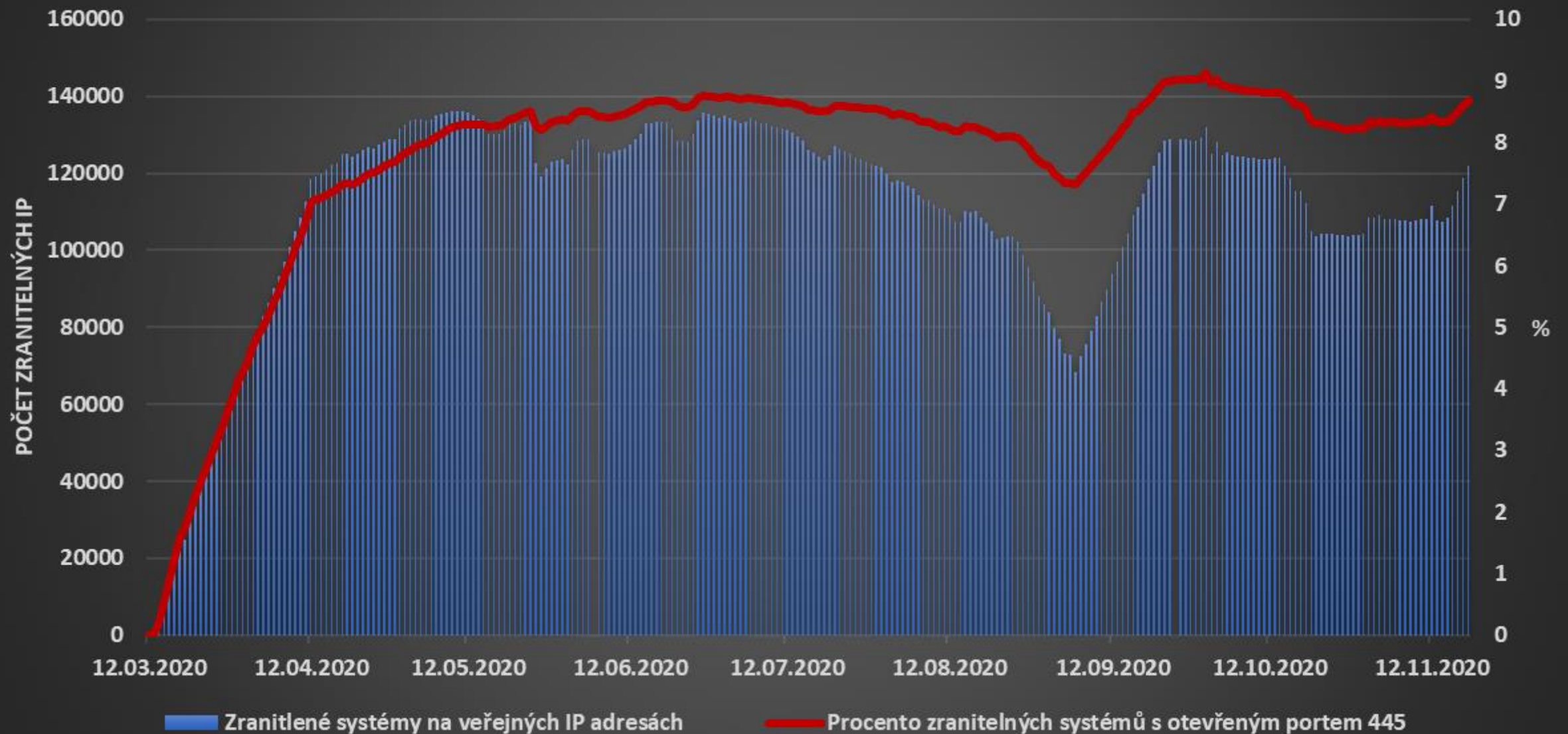
BlueKeep - ČR



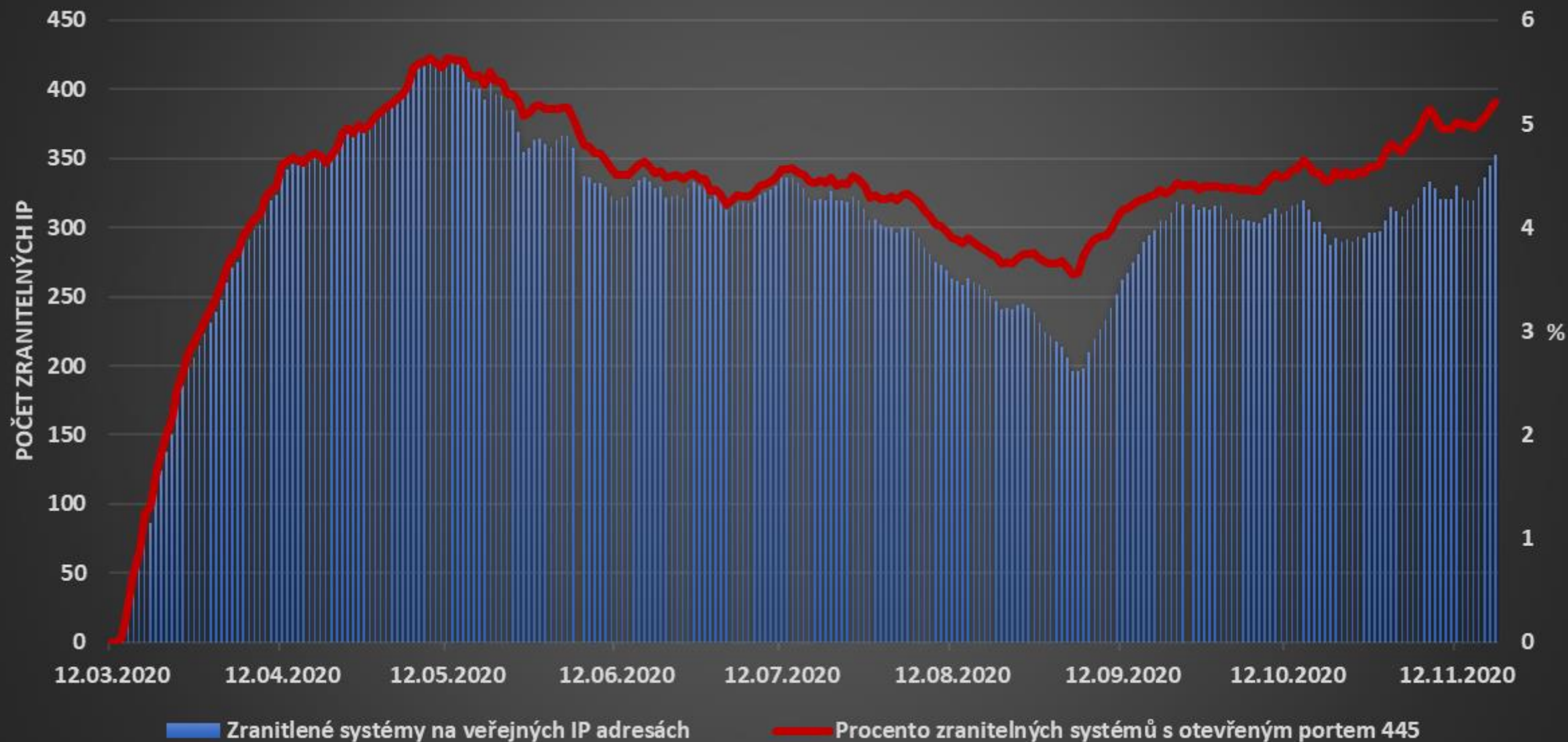
To je ale dávná historie...

- SMBGhost (CVE-2020-0796)
 - Buffer overflow ve zpracování komprimovaných dat v SMBv3
 - CVSS 10.0
 - Zápata publikována (out-of-band) v březnu 2020
 - Postihuje Windows 10 a Windows Server (1903 a 1909)
 - Exploity pro LPE publikovány velmi rychle
 - Exploit pro RCE publikován v červnu 2020

SMBGhost - globální detekce



SMBGhost - detekce v ČR



SMBGhost - detekce v SR



Na co se tedy zaměřit?

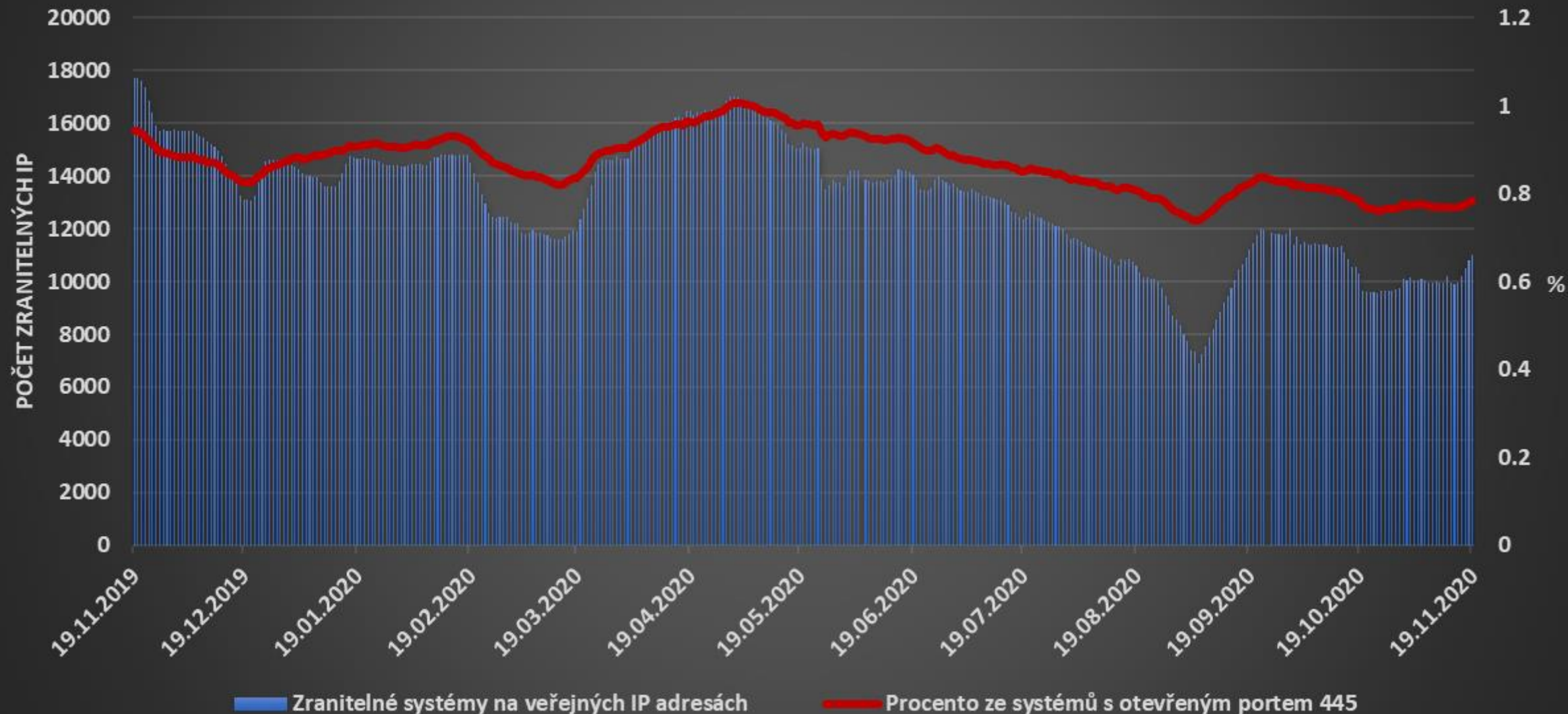
- Formalizovaný patch management
- Ověřování aplikace záplat skrz periodické skeny zranitelností
- Objektivní pohled na aktuální situaci

Hackers

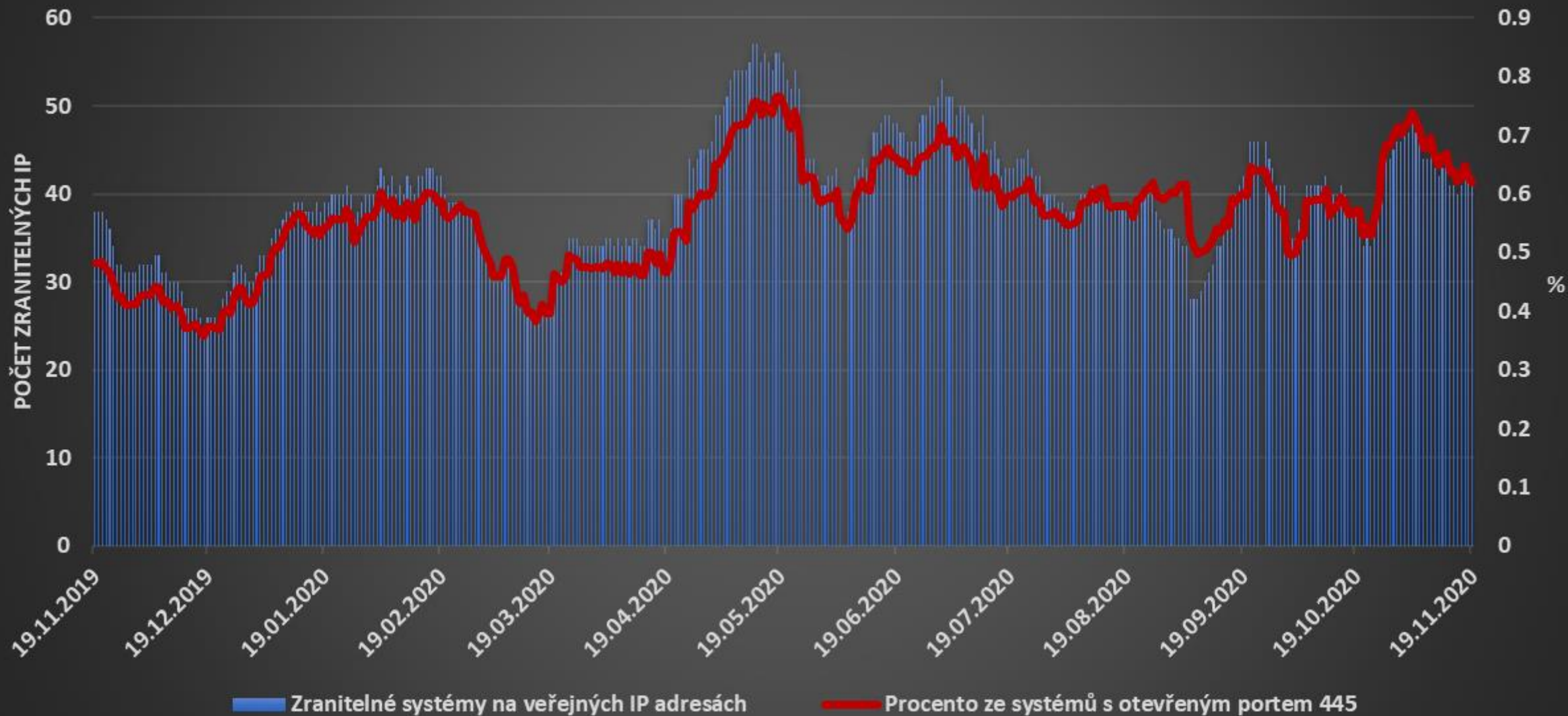
don't give a :

- ☐ About your project's scope
- ☐ It's managed by a third party
- ☐ It's a legacy system
- ☐ It's "too critical to patch"
- ☐ About your outage windows
- ☐ About your budget
- ☐ You've always done it that way
- ☐ About your Go-Live Date
- ☐ It's only a pilot/proof of concept
- ☐ About Non-Disclosure Agreements
- ☐ It wasn't a requirement in the contract
- ☐ It's an internal system
- ☐ It's really hard to change
- ☐ It's due for replacement
- ☐ You're not sure how to fix it
- ☐ It's handled in the Cloud
- ☐ About your Risk Register entry
- ☐ The vendor doesn't support that configuration
- ☐ It's an interim solution
- ☐ It's [insert standard here] compliant
- ☐ It's encrypted on disk
- ☐ The cost benefit doesn't stack up
- ☐ "Nobody else could figure that out"
- ☐ You can't explain the risk to "The Business"
- ☐ You've got other priorities
- ☐ About your faith in the competence of your internal users
- ☐ You don't have a business justification
- ☐ You can't show Return on Investment
- ☐ You contracted out that risk

EtenalBlue - Globální detekce

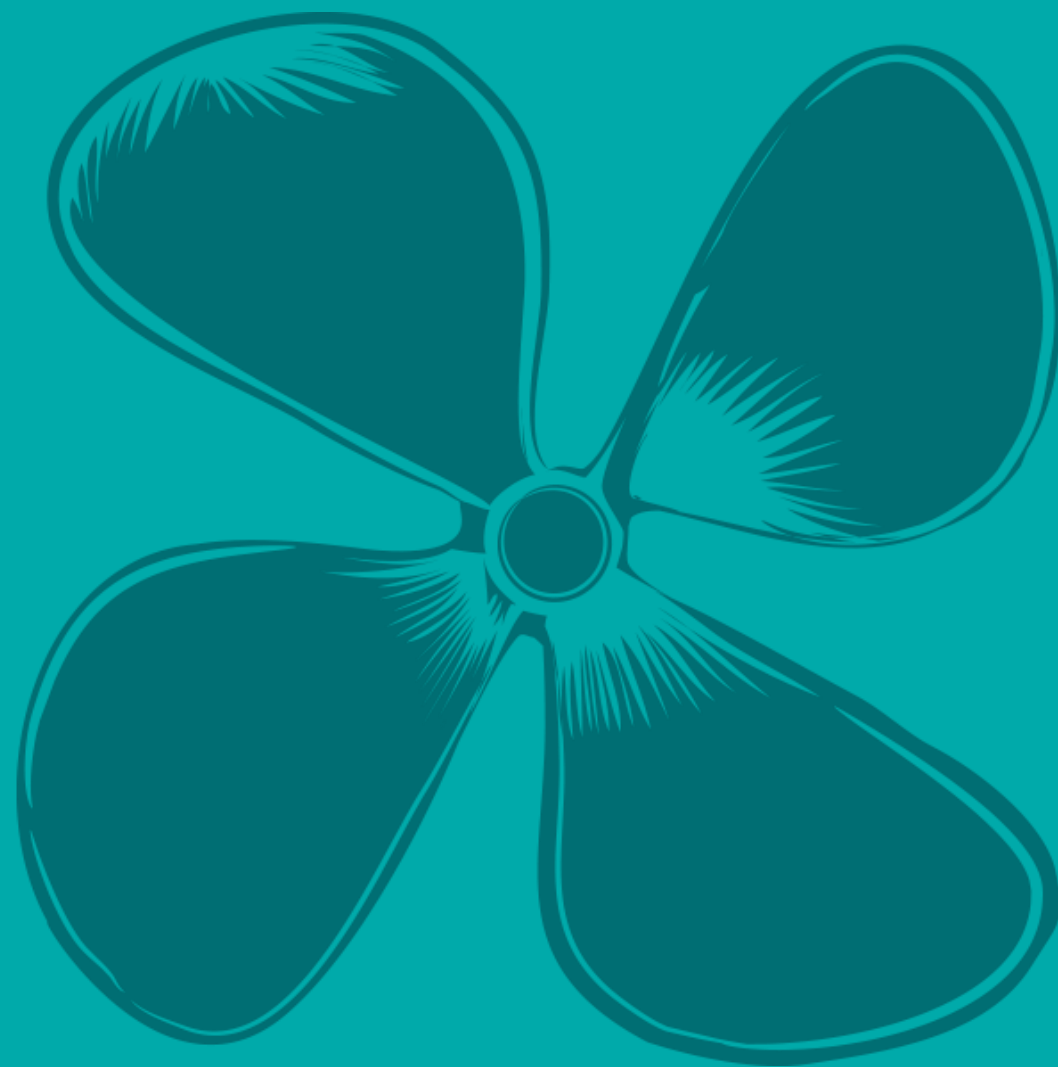


EtenalBlue - ČR



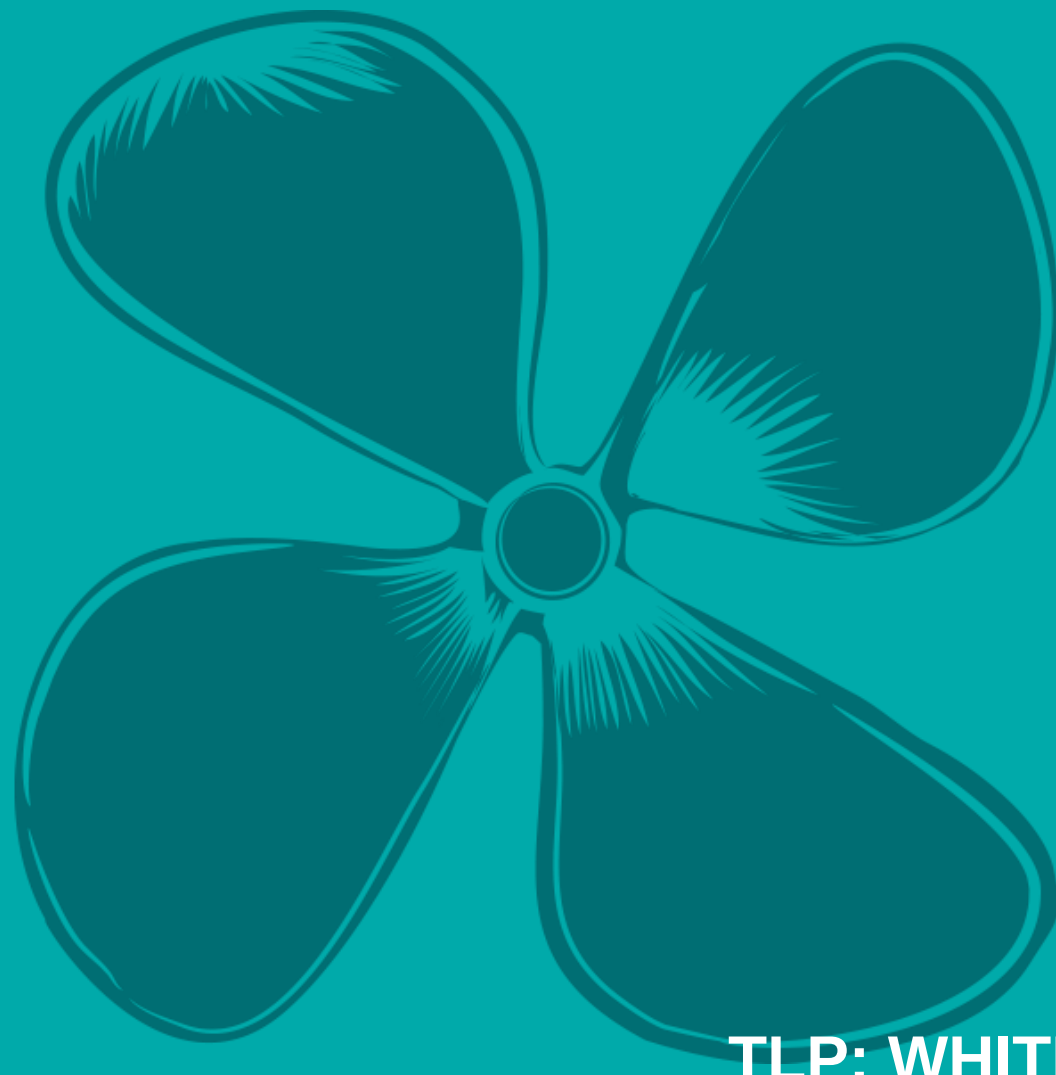
X ALEF

**Prostor pro Vaše
dotazy**



X ALEF

**Děkuji Vám za
pozornost**



TLP: WHITE