



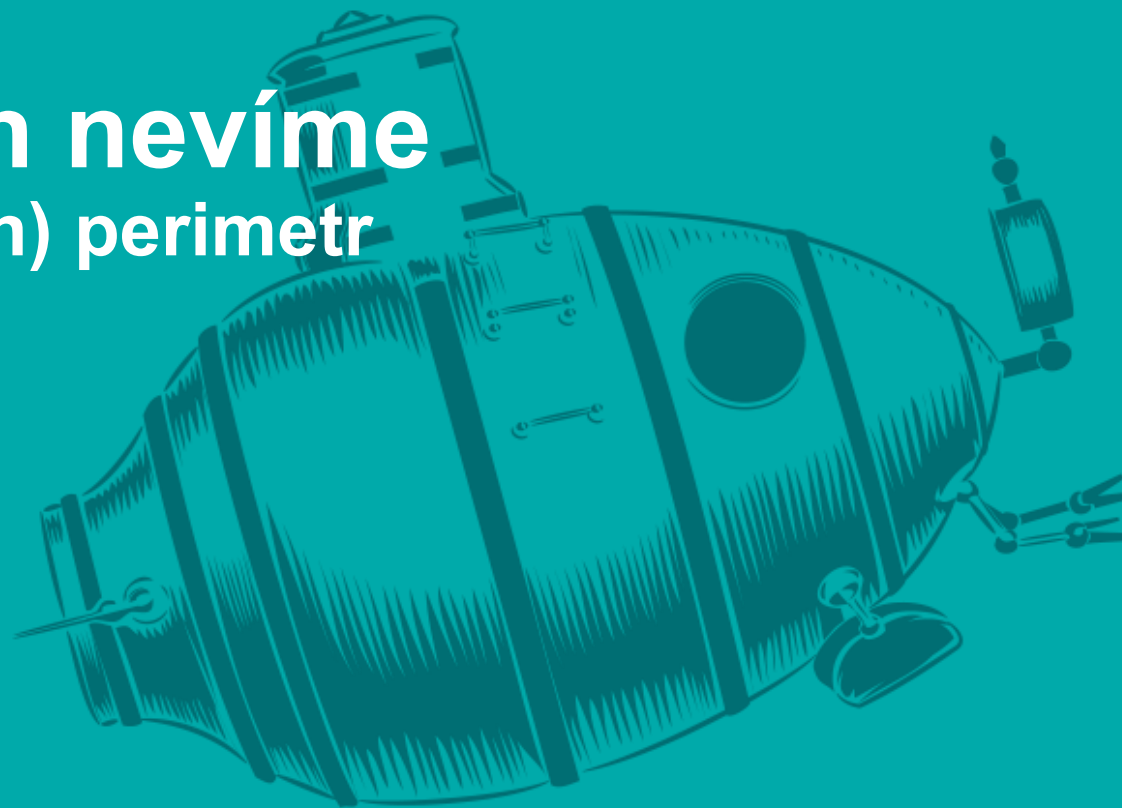
Zranitelnosti, o kterých nevíme

...aneb jak a proč testovat (nejen) perimetr

Jan Kopřiva

jan.kopriva@alef.com

ALEF CSIRT



Obvyklý stav

- Politika – „pravidelné záplatování v návaznosti na kritičnost zranitelnosti“
- Realita
 - Chybí katalog aktiv/CMDB
 - „Co je kritické nám řekne vendor“
 - Nejsou stanovená konfigurační/patchovací okna

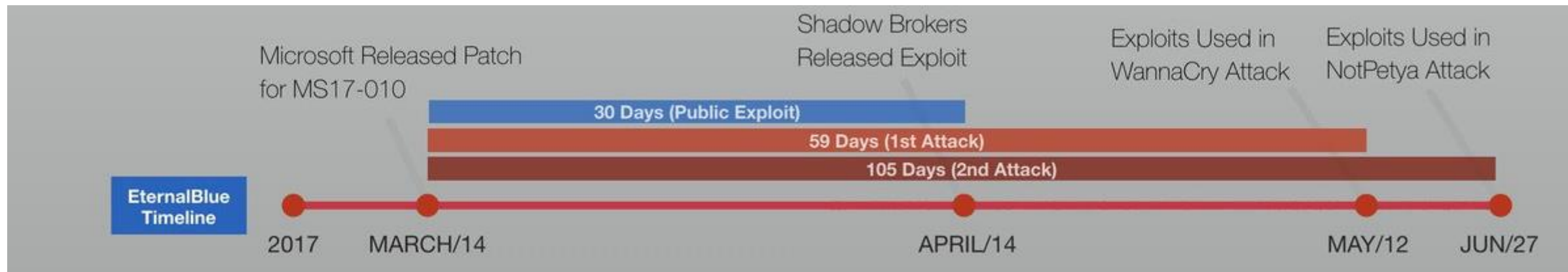
=> Nevíme, jaké zranitelnosti nám (nejen) v perimetru zůstávají

Je to velký problém?

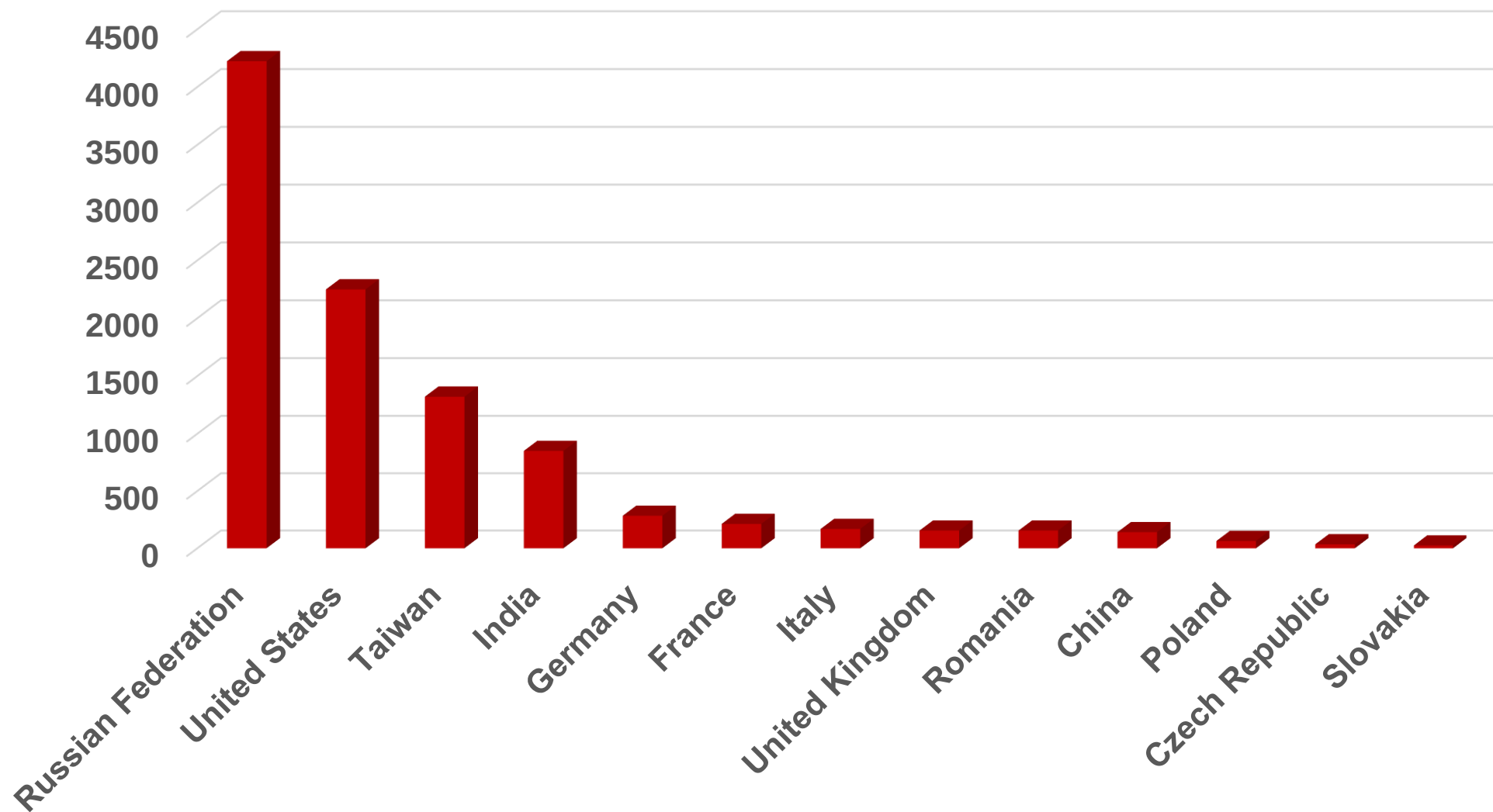


EternalBlue

- Exploit vyvinutý NSA
- RCE ve zpracování SMBv1
- Zcizený a publikovaný Shadow Brokers

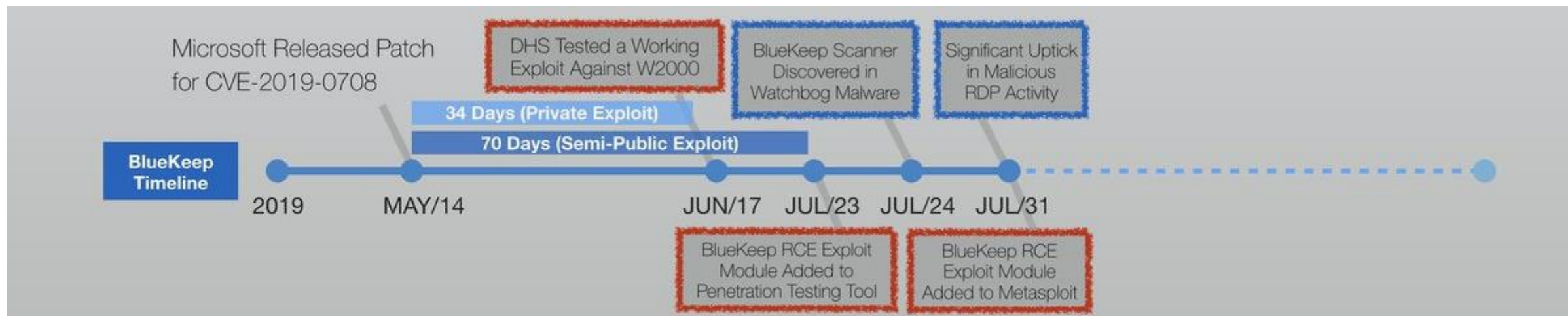


EternalBlue – počty zranitelných systémů

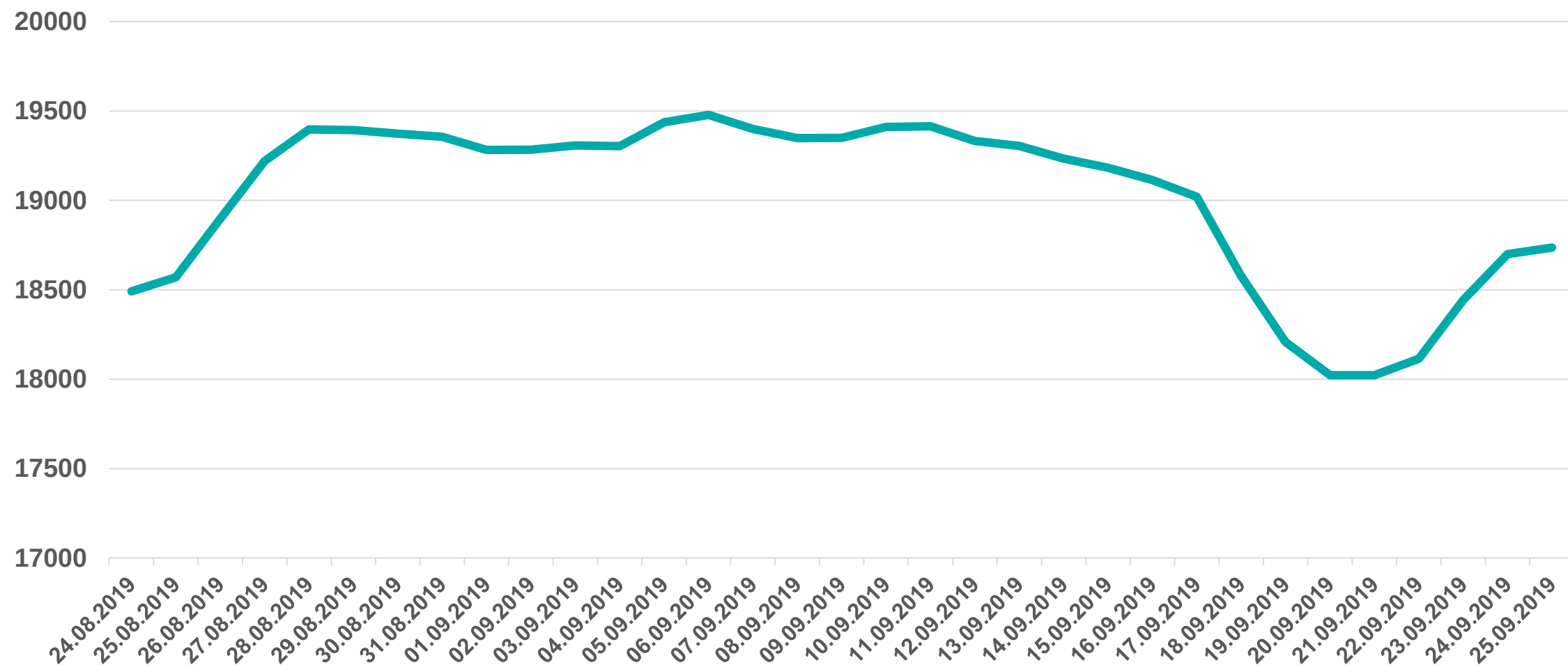


BlueKeep

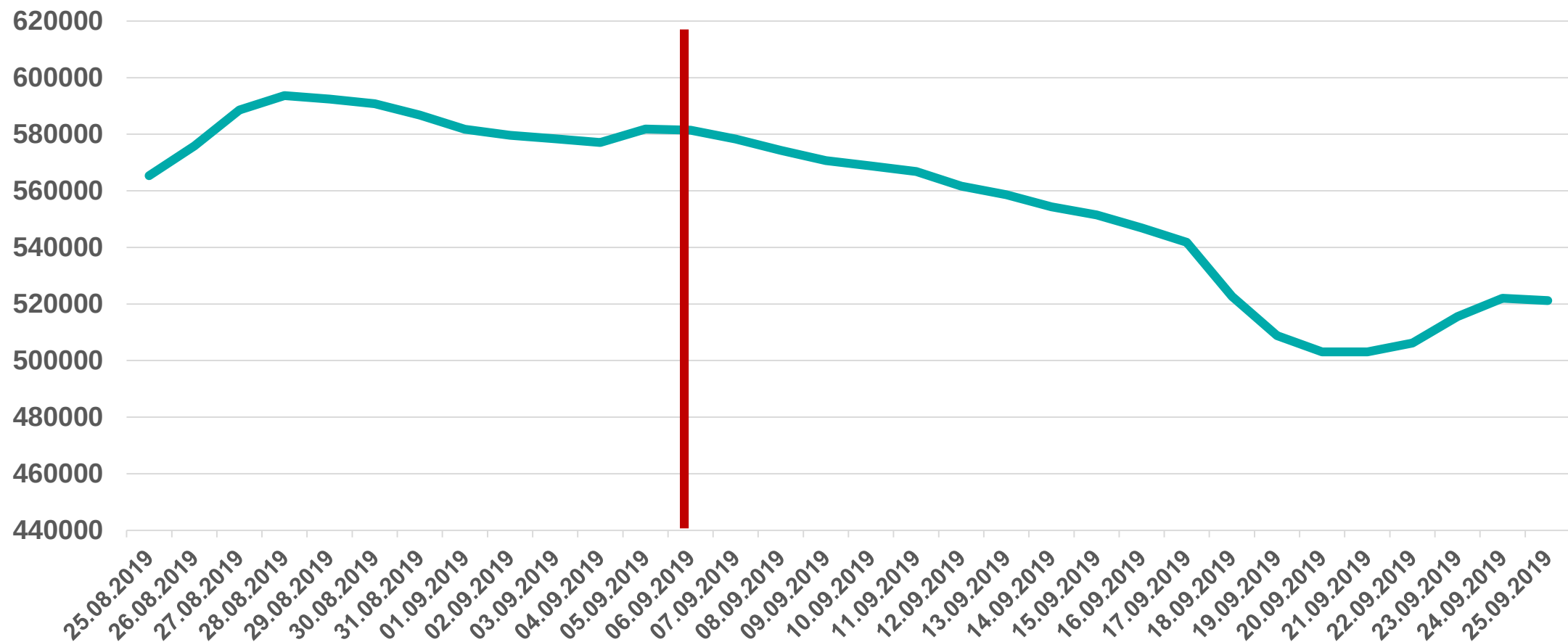
- RCE zranitelnost v RDP
- Možnosti zneužití v podstatě totožné s EternalBlue



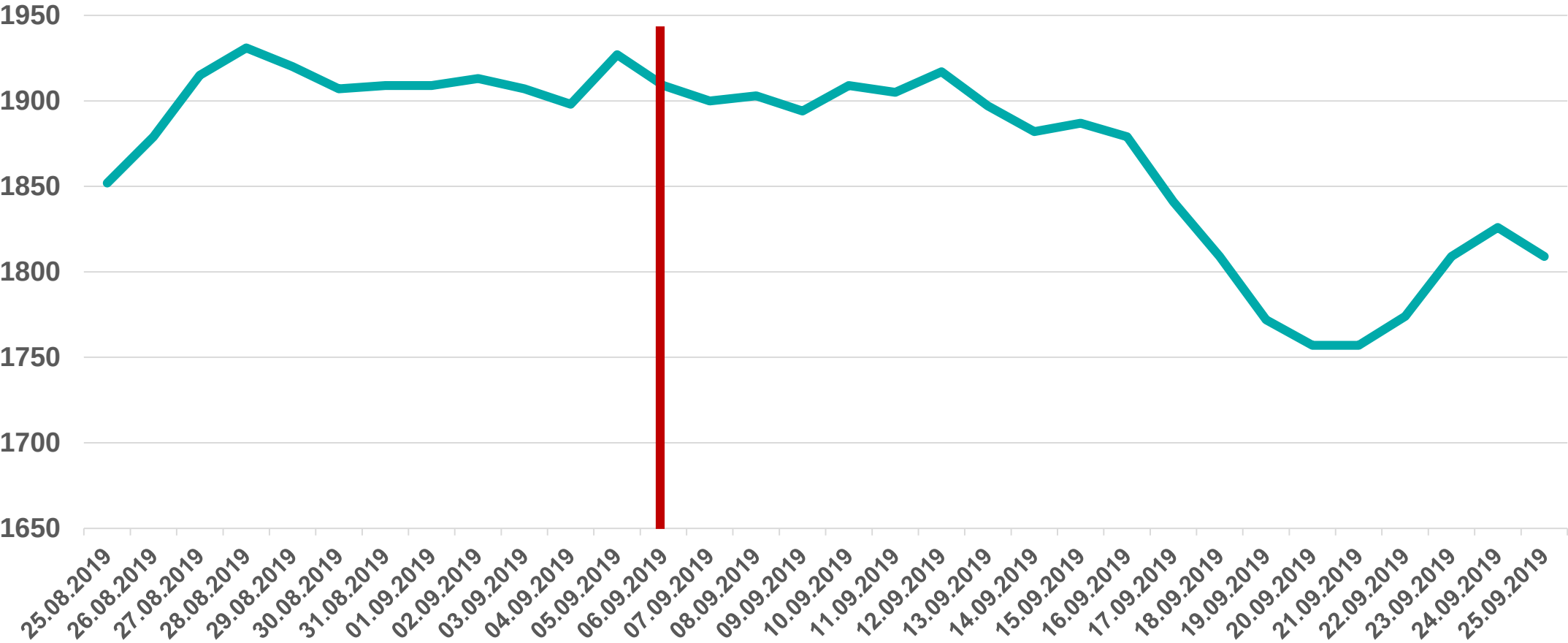
RDP v CZ



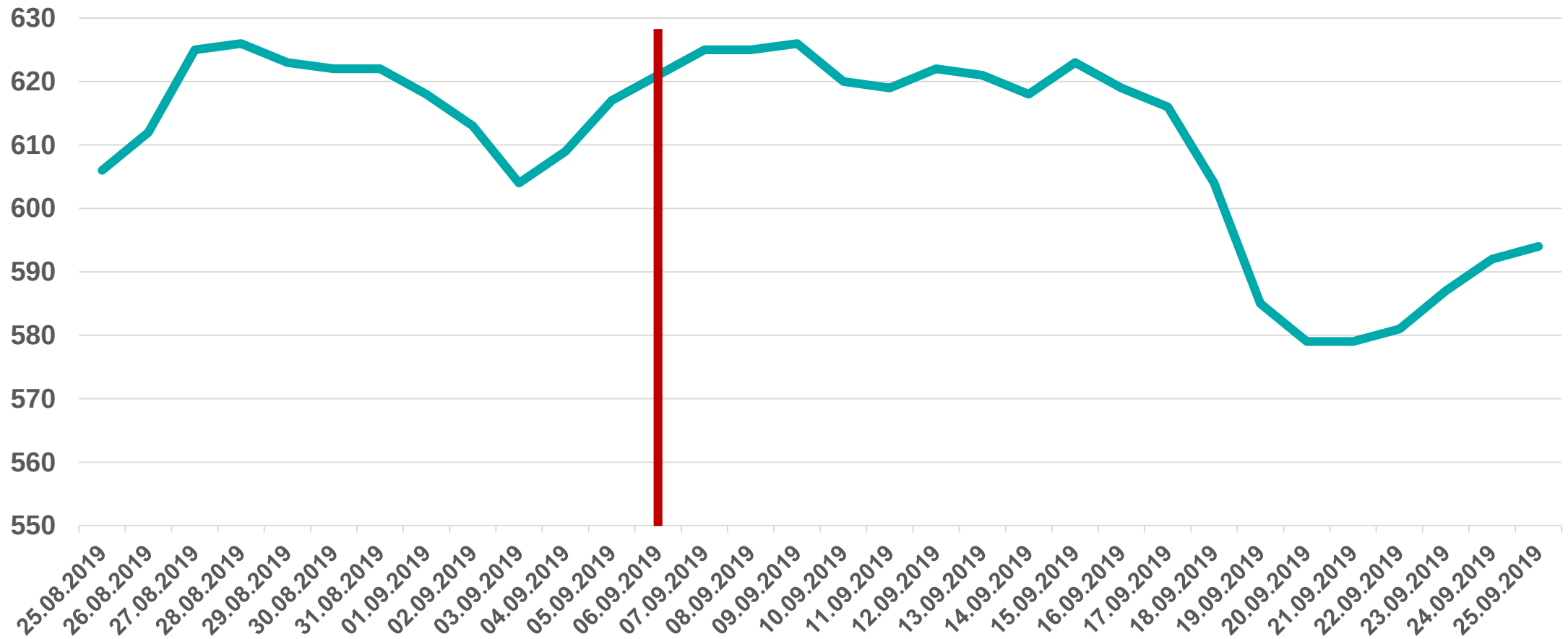
BlueKeep – globální vývoj



BlueKeep – CZ



BlueKeep – SK



DejaBlue

- RCE zranitelnost v RDP
- Možnosti zneužití v podstatě totožné s EternalBlue
- Zranitelné všechny moderní verze Windows



Co z toho plyne?

- Podobných zranitelností není málo a útok typu WC se může objevit zítra
- Spoléhat na to, že „patchování funguje jak má“ nestačí
 - Absenci zranitelností je nutné ověřovat

Penetrační testy a Vulnerability assessmenty

	Vulnerability assessment	Penetrační test
Zaměření	Detekce známých zranitelností	Identifikace známých i neznámých zneužitelných zranitelností
Provedení	Automatizované	Převážně manuální
Frekvence	Zpravidla vysoká (např. 1x za týden, případně kontinuálně)	Zpravidla nízká (např. 1x za rok a při změnách)
Nutná znalost	Nízká	Vysoká
Realizace	Většinou interní zdroje	Většinou externí zdroje
Výstup	Chybějící záplaty a konfigurační nedostatky	Reálně využitelné zranitelnosti

Typy penetračních testů

- Dle zaměření
 - Webové aplikace
 - IT infrastruktura
 - Fyzická bezpečnost
 - Sociální inženýrství
 - A další
 - Mobilní aplikace, IoT, Wi-Fi, SIP,...

Jak začít?

- Formalizace požadavků na bezpečnostní testování
- Formalizace požadavků na záplatování
- Časté/pravidelné vulnerability skeny
 - S pomocí interních zdrojů, nebo aaS
 - Nevyžadují vysokou vyspělost řízení IT, ani ISMS

Jak pokračovat?

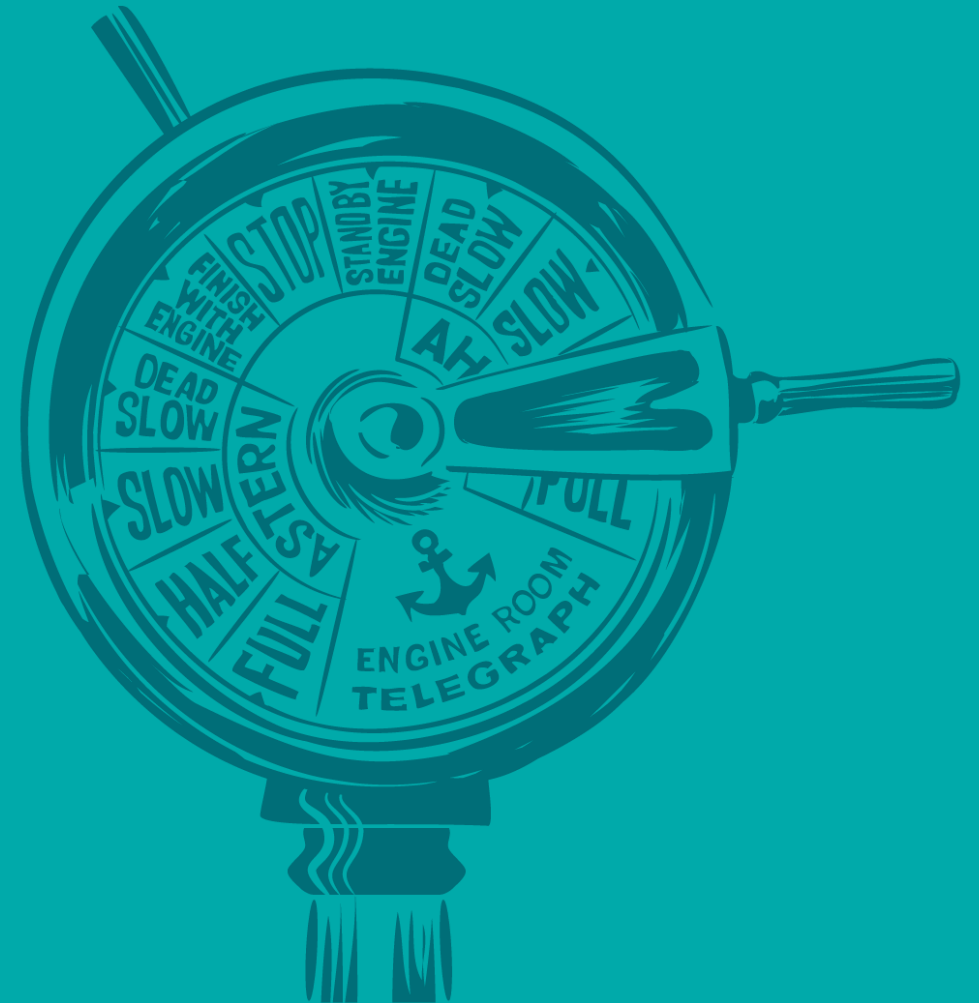
- Sledování vývoje zranitelností a hrozeb
- Pravidelné/ad-hoc realizované penetrační testy
 - Rozsah a typ dle formalizovaných požadavků
 - Nezapomínat na testování lidského faktoru
 - Socioinženýrské a fyzické testy

Na co nezapomenout?

- Nesoustředíme se jen na perimetr
 - Phishing a útoky skrze dodavatelský řetězec perimetr překonají velmi snadno

X ALEF

Q&A



X ALEF

**Děkuji Vám za
pozornost**

