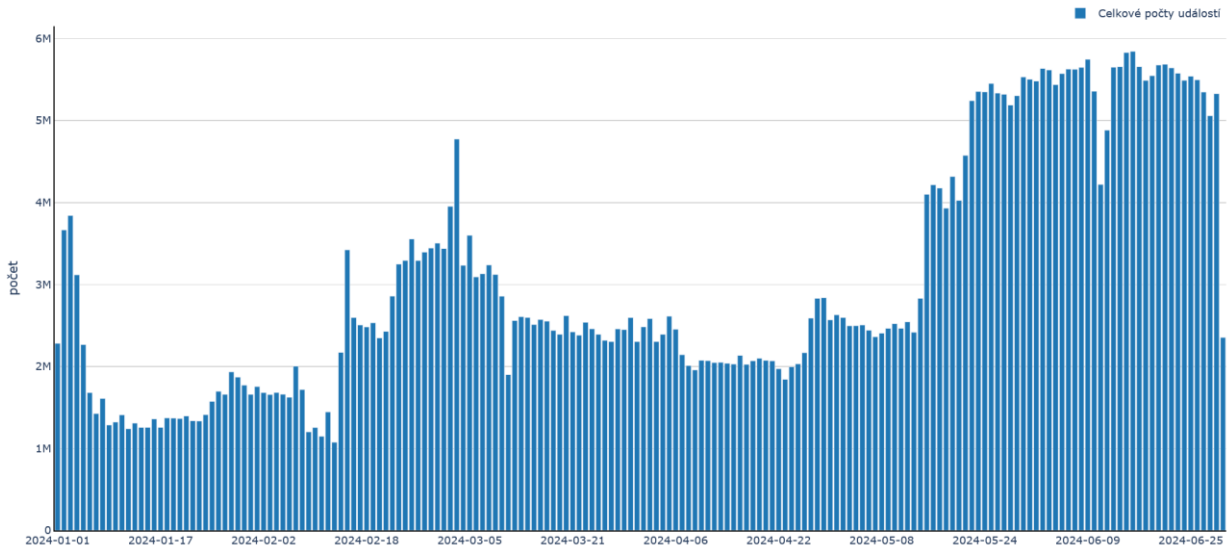
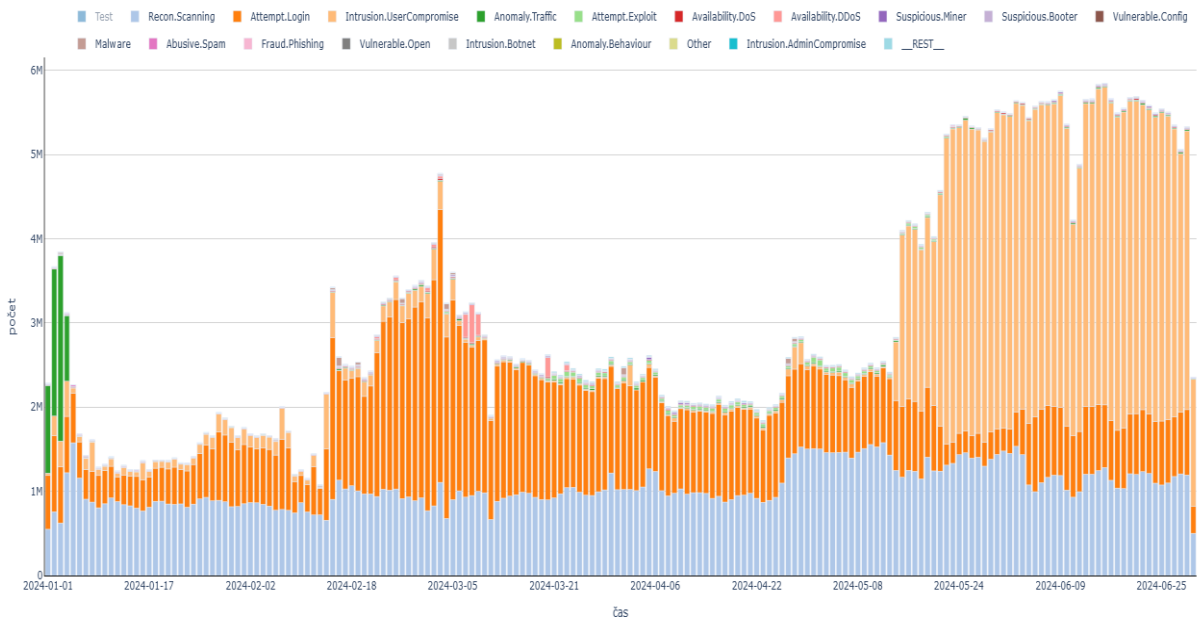
Bezpečnostní incidenty v akademických sítích sítě CESNET v 1. pololetí 2024.

V 1. pololetí 2024 bylo v systému Mentat spravovaném bezpečnostním týmem CESNET-CERTS evidováno *51 959* statistických záznamů s *555 394 982* bezpečnostními událostmi zaznamenanými v síti CESNET (Obr. 1). K většině událostí došlo v tzv. *externích* sítích, tj. takových, které se uživatelů sítě CESNET přímo netýkají. *Interních*, převážně akademických sítí se týkala jen 2% (*9 716 812*) událostí (Obr. 4).



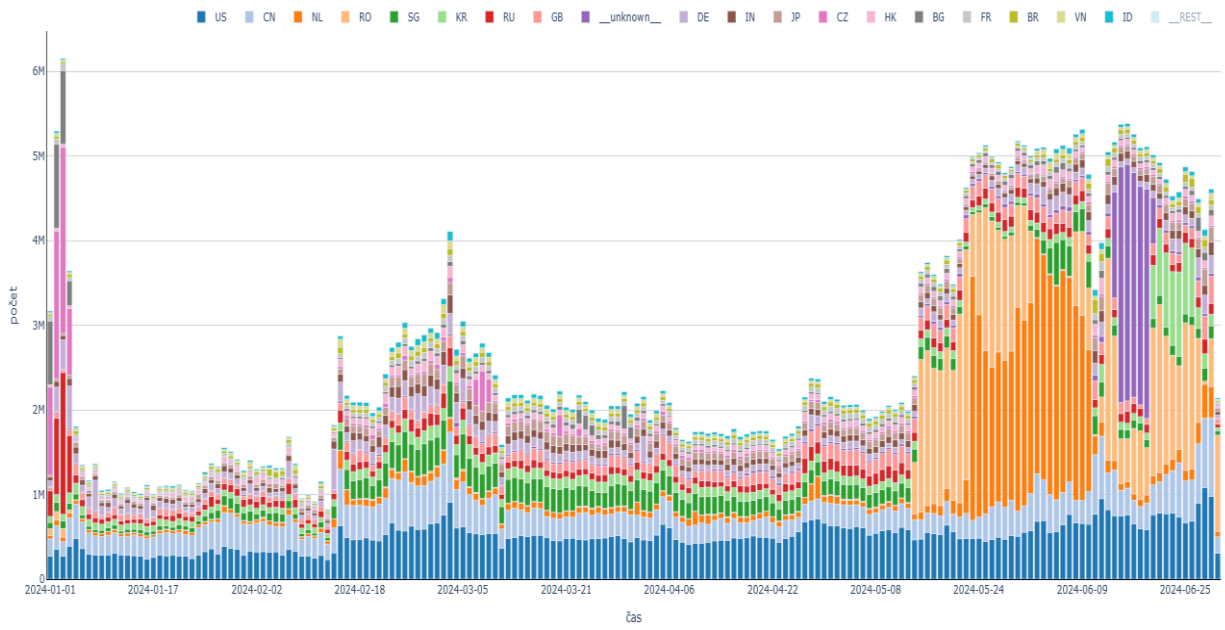
Obr. 1. Časová osa bezpečnostních incidentů v síti CESNET v 1. pol. 2024

Ve zprávě *Kybernetické incidenty pohledem NÚKIB - leden 2024* je uvedeno, že v lednu 2024 došlo pouze k mírnému navýšení incidentů oproti prosinci 2023. Na rozdíl tomu data v systému Mentat vykazují v prvních třech dnech ledna výrazně zvýšenou aktivitu, ale pouze v kategorie nízké závažnosti (*AnomalyTraffic)*. K dalšímu vzestupu aktivity dochází až v polovině února s maximem v začátku března (kategorie *Attempt.Login*). Velmi výrazný vzrůst událostí je však evidován od poloviny května až do konce sledovaného období (kategorie *Inrusion.UserCompromise*). Během celého období lze pak pozorovat prakticky konstantní skenování portů síťových zařízení (kategorie *Recon.Scanning*). (Obr.2).



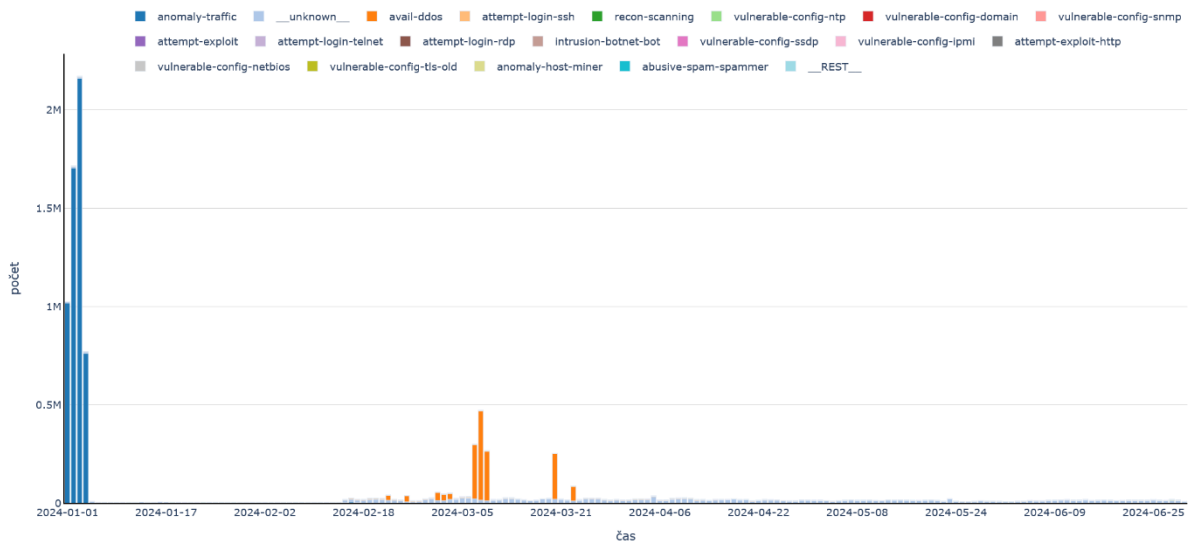
Obr. 2. Časová osa kategorií bezpečnostních incidentů v síti CESNET v 1. pol. 2024

Podrobnější analýza ukázala, že bezpečnostní události v začátku roku mají původ v Rusku, ČR a Bulharsku. Naproti tomu události registrované od poloviny května mají původ v Holandsku a Rumunsku, částečně i v Korei. (Obr.3.)



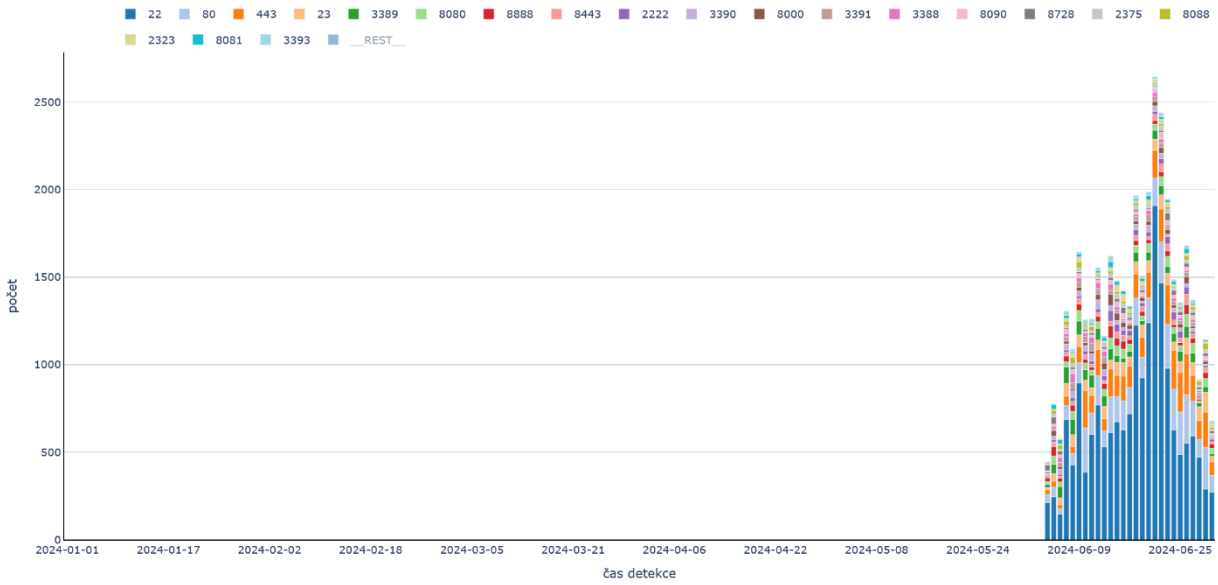
Obr. 3. Časová osa bezpečnostních incidentů v síti CESNET v 1. pol. 2024 podle země jejich původu

V *interních sítích* patřila aktivita v začátku roku opět do kategorie nízké závažnosti *(AnomalyTraffic)*. Z kategorie závažných bezpečnostních událostí byl pak zaznamenán pouze jeden DDoS útok na síť vutrb.cz v době od 6.3. do 8.3. (Obr. 4).



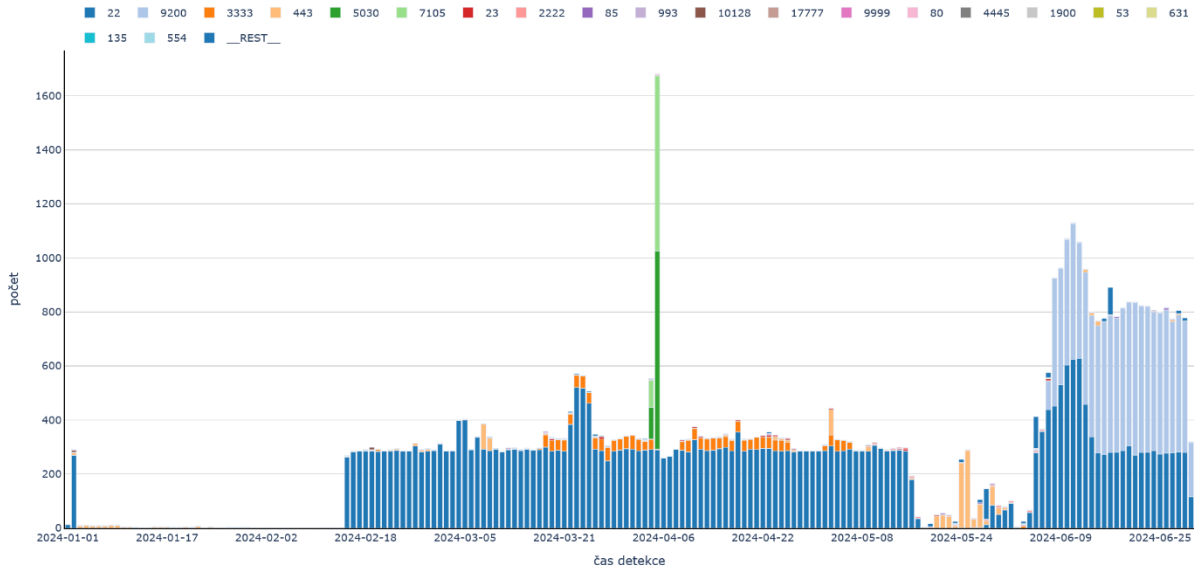
Obr.4 . Časová osa kategorií bezpečnostních incidentů v interních sítích sítě CESNET v 1. pol. 2024

V síti AV ČR (*adresový rozsah 147.231.0.0/16*) bylo v červnu 2024 zaznamenáno 112 744 událostí v kategoriích *Recon.Scanning, Anomaly.Traffic a Attempt.Login* směrovaných zvenčí na porty 22, 80, 443. V ostatních měsících byl počet událostí zanedbatelný. (Obr. 5)



Obr.5 Časová osa kategorií bezpečnostních incidentů směrovaných do sítě AV ČR v 1. pol. 2024

Síť AV ČR byla ve sledované období také zdrojem *1 007 612* bezpečnostních událostí nejčastěji v kategoriích *Anomaly.Traffic a Attempt.Login*. Cílem byly zejména porty 22 a 9200 (0br. 6) Mimo to bylo v této síti zaznamenáno *24* případů porušení autorských práv sdílením autorských děl - filmů v platformě BitTorrent.



Obr.6 Časová osa cílených portů ze sítě AV ČR v 1. pol. 2024