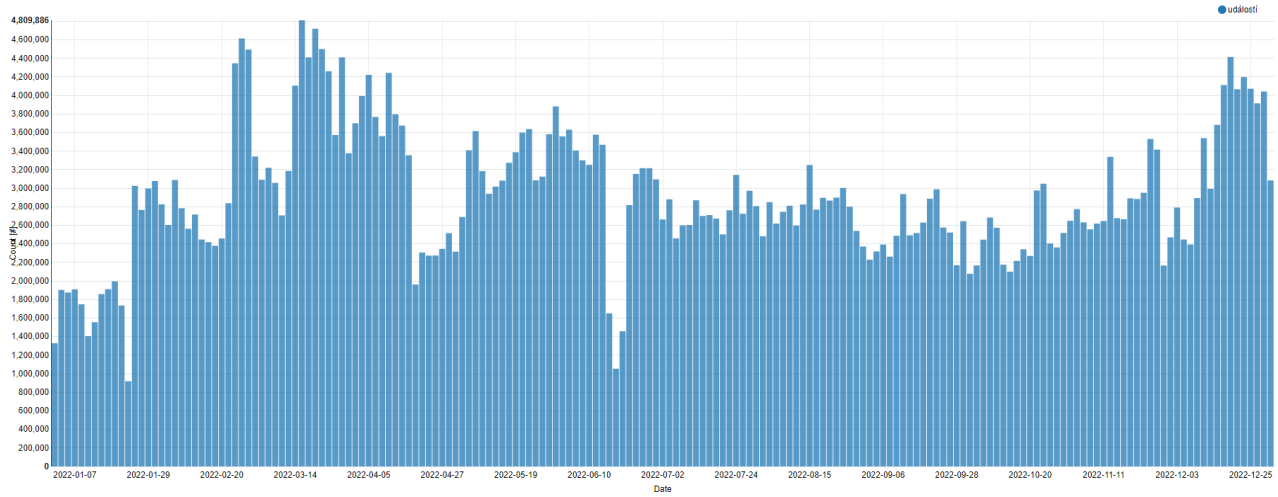
Bezpečnostní události v akademických sítích CESNET v roce 2022

Bezpečnostní tým sítě AV ČR CAS-CSIRT zaznamenává a společně se správci sítí jednotlivých pracovišť řeší bezpečnostní události v síti AV ČR již od roku 2018. Od poloviny roku 2021 pak sleduje i incidenty v rozsahem podobných akademických sítích ČVUT a UK a pro porovnání i v celé síti CESNET.

Tato studie pojednává o bezpečnostních událostech detekovaných v akademických sítích CESNET po dobu jednoho roku od 1. 1. 2022 do 31. 12. 2022 a registrovaných v systémech **Mentat** a **Warden** spravovaných bezpečnostním týmem CESNET-CERTS.

Za roční období od 1. 1. 2022 do 31. 12. 2022 bylo v systému **Mentat** registrováno **105 039** záznamů s více než **532mil.** bezpečnostními událostmi zaznamenanými v sítích CESNET. Z toho více než **27mil.** událostí se týkalo sítě AV ČR a z nich přibližně **3mil.** byly v síti AV ČR iniciovány.

a) Bezpečnostní události v celé síti Cesnet

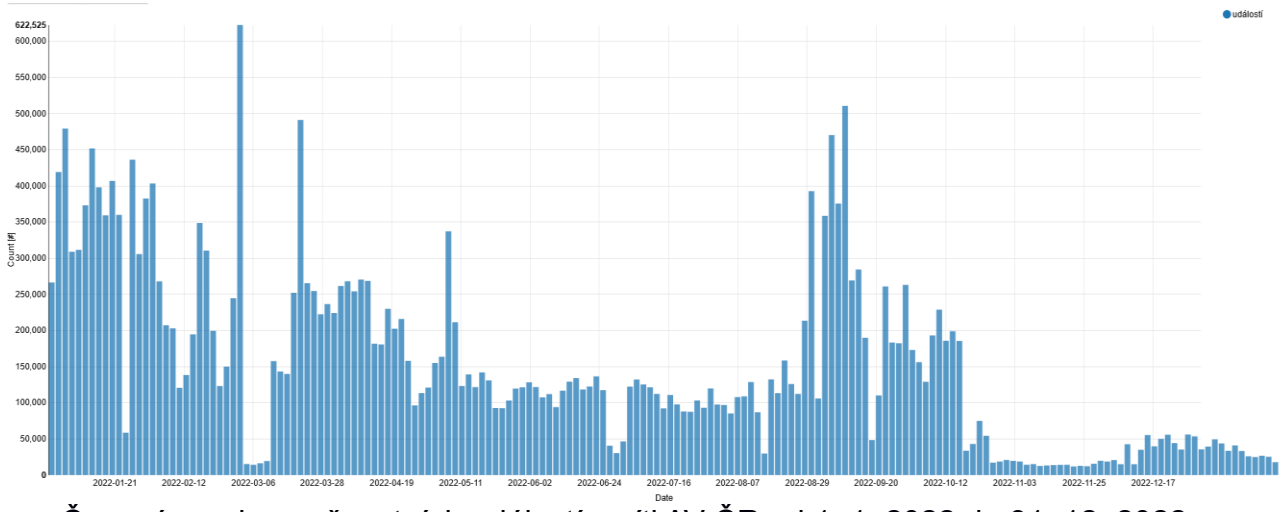


Časová osa bezpečnostních událostí zaznamenaných v síti Cesnet
od 1. 1. 2022 do 31. 12. 2022

Na obrázku je zřejmý výrazný nárůst bezpečnostních událostí v 1. čtvrtletí 2022, který je možné dát do souvislosti se začátkem konfliktu na Ukrajině. Na konci 4. čtvrtletí je nápadná koincidence bezpečnostních událostí pravděpodobně s vánočními svátky.
Tento výsledek je v dobrém souladu se Zprávou o stavu kybernetické bezpečnosti ČR za rok 2022 vydanou NÚKIB 17.3.2023, která zvýšenou aktivitu v 1. čtvrtletí přičítá ruskojazyčným haktivistickým skupinám Killnet a Anonymous Russia. NÚKIB zároveň dovozuje, že útoky obou skupin téměř jistě souvisely s českou podporou Ukrajiny.

Podrobnější analýza ukázala, že z bezpečnostních událostí zaznamenaných v sítích CESNET byly nejčastější pokusy o neoprávněné připojení k cizímu počítači protokolem ssh (*Attempt-Login-ssh - 55,05 %)* a skenování portů cizích počítačů (*Recon-Scanning - 32,43 %)*, které zřejmě poskytuje útočníkům základní informace o zranitelných a teoreticky dostupných systémech připojených do sítě Internet.

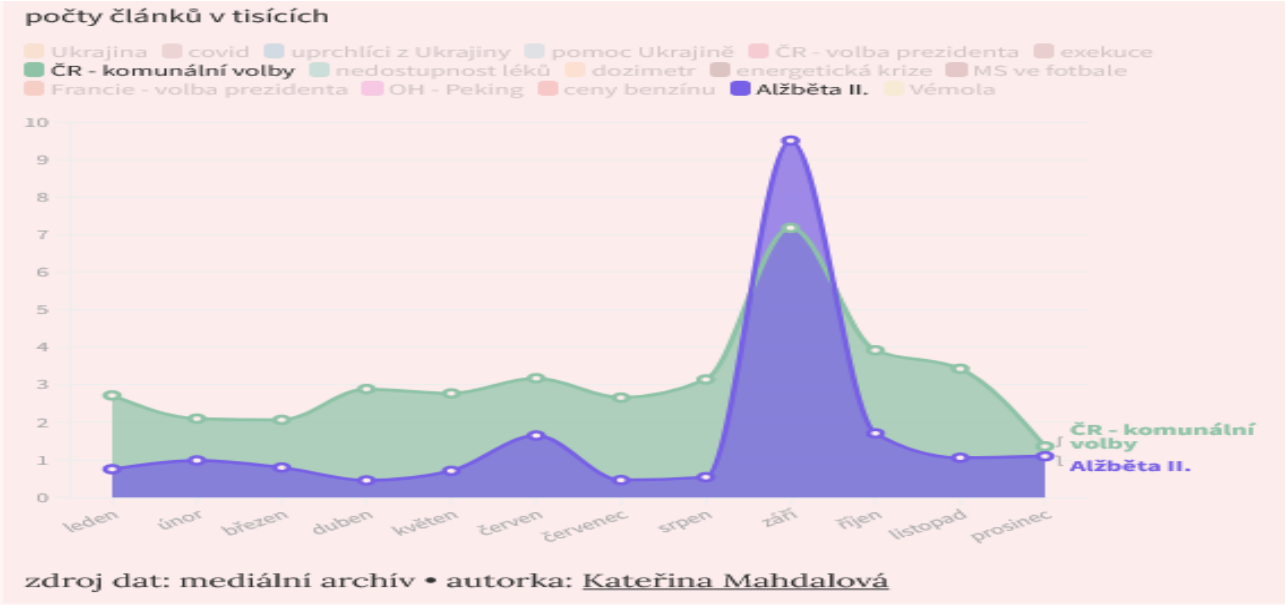
b) Bezpečnostní události v síti AV ČR



Časová osa bezpečnostních událostí v síti AV ČR od 1. 1. 2022 do 31. 12. 2022

Obrázek zobrazuje časovou osu bezpečnostních událostí zaznamenaných v síti Cesnet, ale týkajících se sítě AV ČR v období od 1. 1. 2022 do 31. 12. 2022. Zahrnuje události směrované do sítě AV ČR i události iniciované v síti AV ČR. Časová osa má zcela odlišný charakter od časové osy z Obr. 1. To naznačuje, že bezpečnostní události zaznamenané v celé síti Cesnet odráží jiné časové mezníky než události vztažené pouze k síti AV ČR. Například výrazné zvýšení počtu incidentů v září 2022 koinciduje s počtem článků v českých mediích k aktuálním událostem, konkrétně k úmrtí královny Alžběty II.

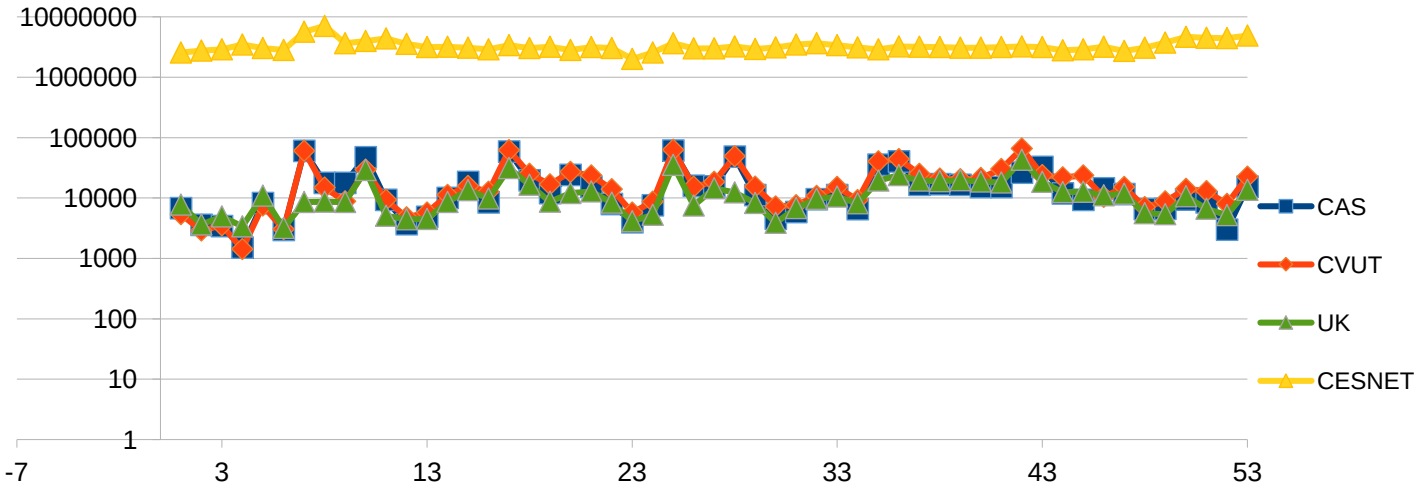
Na rozdíl od událostí v síti Cesnet byl v síti AV ČR nejčastější blíže neurčený podezřelý provoz (*Anomaly-traffic - 70,21 %)* většinou související s různými testy a pak nespecifikované události např. Malware, šíření škodlivých kódů *25,71 %)*



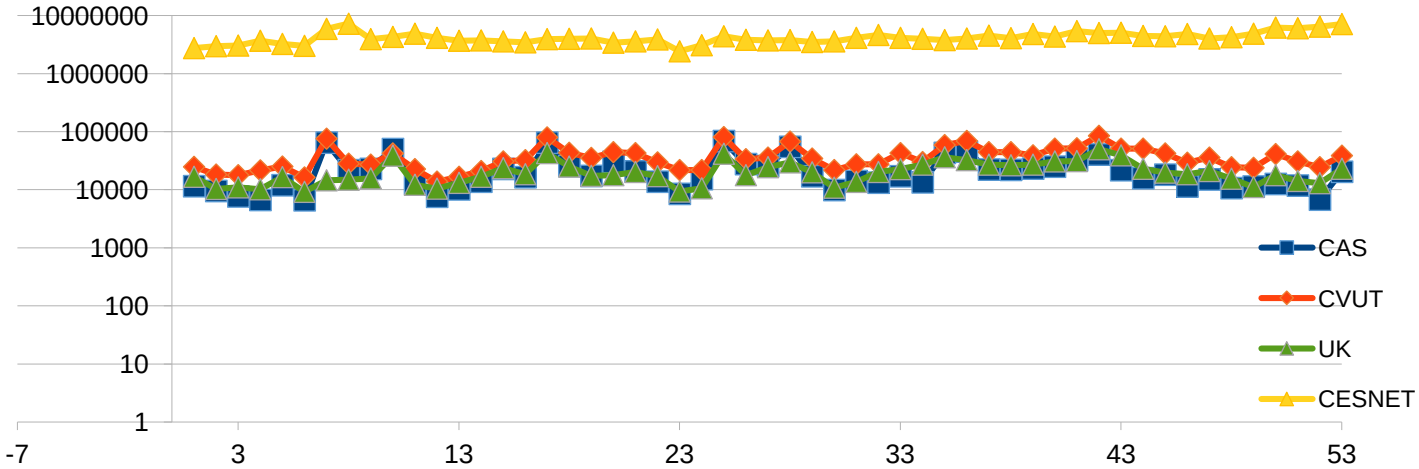
Počty článků k významným událostem v roce 2022 uveřejněných v českých médiích.

Závažnost všech bezpečnostních událostí byla podle stupnice bezpečnostního týmu CESNET-CERTS klasifikována jako nízká a to jak u událostí v síti Cesnet (*87,20 %,)* , tak i u událostí v síti AV ČR (*73,48 %*).

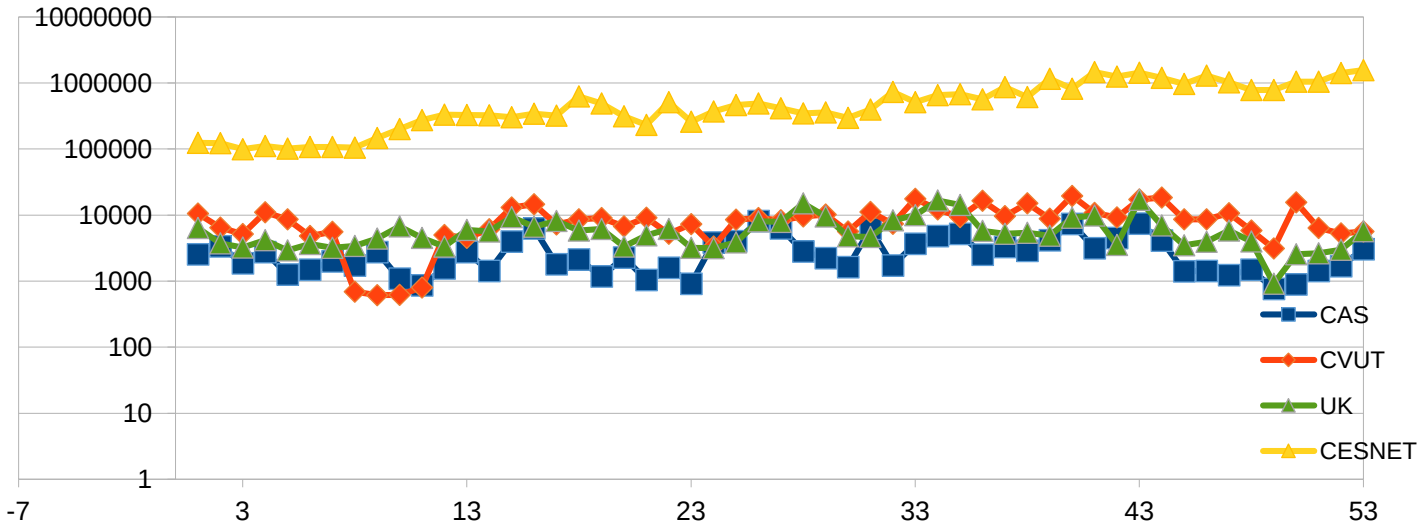
Zpracování bezpečnostních událostí získaných prostřednictvím systému Warden v zásadě potvrdilo výsledky získané z dat Mentat, navíc umožnilo i podrobnější srovnání bezpečnostních incidentů v sítích ČVUT a UK, kdy ukázalo na jejich vzájemnou korelaci. V celkovém množství je opět vidět zvýšená aktivita po napadení Ukrajiny.



Časové řady týdenních počtů bezpečnostních incidentů v roce 2022



Časové řady týdenních počtů bezpečnostních incidentů typu *Recon Scanning* v roce 2022 kopírují jejich celkové počty (viz předchozí obrázek).
Události typu *Recon Scanning* byly nejčastější a od konce roku 2021 byly cíleny na velké množství adres zároveň. Zdroje těchto hromadných útoků byly podle IP adres lokalizovány v Moskvě.

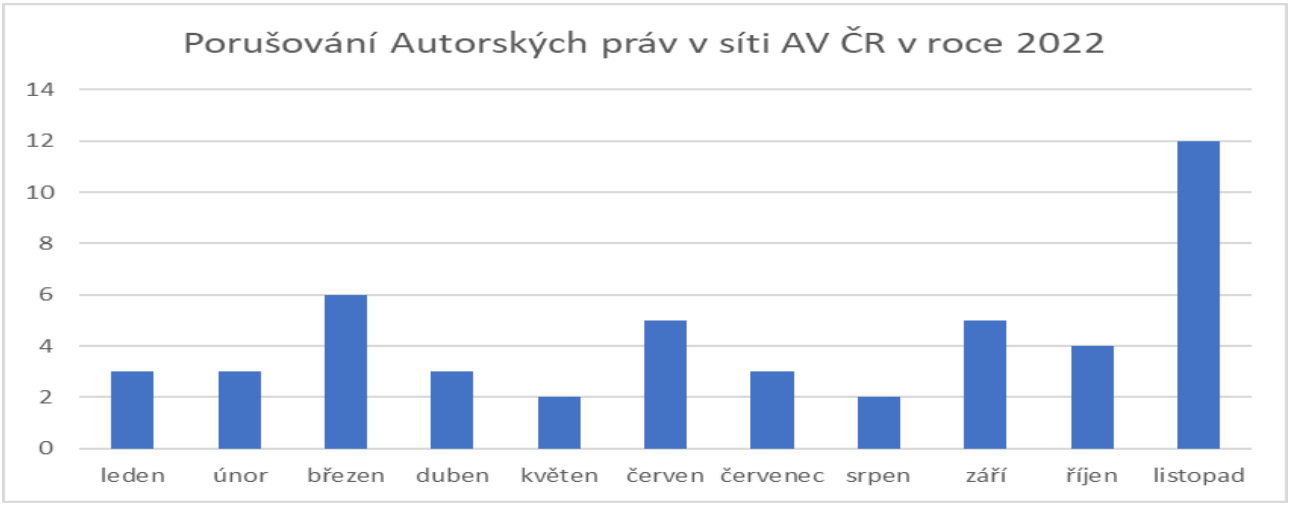


Časové řady týdenních počtů bezpečnostních incidentů typu *Attempt Login* v roce 2022

Časové řady týdenních počtů bezpečnostních incidentů typu *Attempt Login* v roce 2022 v akademických sítích vykazují mírný růst. Výrazný a setrvalý růst lze však pozorovat v síti Cesnet.

Porušování autorských práv v síti AV ČR

V roce 2022 bylo v síti AV ČR zaznamenáno 48 případů porušení autorských práv. Docházelo k němu ve všech případech neoprávněným šířením filmů v síti *BitTorrent*. Správci lokálních sítí, ve kterých k incidentu došlo byli vždy informováni a vyzváni k tomu, aby uživatele svých sítí upozornili na specifickou vlastnost sítě *BitTorren*t, tj. poskytování segmentů stažených multimediálních záznamů ostatním uživatelům této sítě. I když jejich samotné stažení je legální, lze je chápat jako tzv. Volné užití, následné šíření odporuje autorskému zákonu.
Porušování autorských práv v síti AV ČR v jednotlivých měsících roku 2022 ukazuje následující graf.



Závěr

Cílem této studie bylo bližší poznání bezpečnostních rizik v akademických sítích, zjistit, jaké bezpečnostní incidenty se tu nejčastěji vyskytují a jaké je jejich časové rozložení. Studie také ukázala na korelaci těchto událostí s některými významnými událostmi, kterými bylo v roce 2022 např. zahájení vojenských akcí na Ukrajině nebo úmrtí královny Alžběty II. Také ukázala, že značný počet incidentů je způsoben napadenými a „infikovanými“ počítači v lokálních sítích akademických pracovišť. Ale v poměru k vysoké intenzitě útoků byly reálné škody v sítích zanedbatelné, což svědčí o dobré úrovni bezpečnosti akademických sítí.
Ze závěrů NÚKIB - Zprávy o stavu kybernetické bezpečnosti ČR za rok 2022 navíc plyne, že i v roce 2023 bude kybernetický prostor v ČR do jisté míry i nadále ovlivňován děním na Ukrajině.

Výsledky studie naznačují, že ochrana proti stále sofistikovanějším kybernetickým útokům vyžaduje nejen stále dokonalejší firewally a podobná technická zařízení a značné úsilí správců těchto zařízení ale i zodpovědné chování uživatelů všech, nejen akademických sítí.

Miroslav Indra, Jiří Janáček

Literatura:
NÚKIB 19.7. 2023: Zpráva o stavu kybernetické bezpečnosti ČR za rok 2022
https://mentat.cesnet.cz
https://warden.cesnet.cz