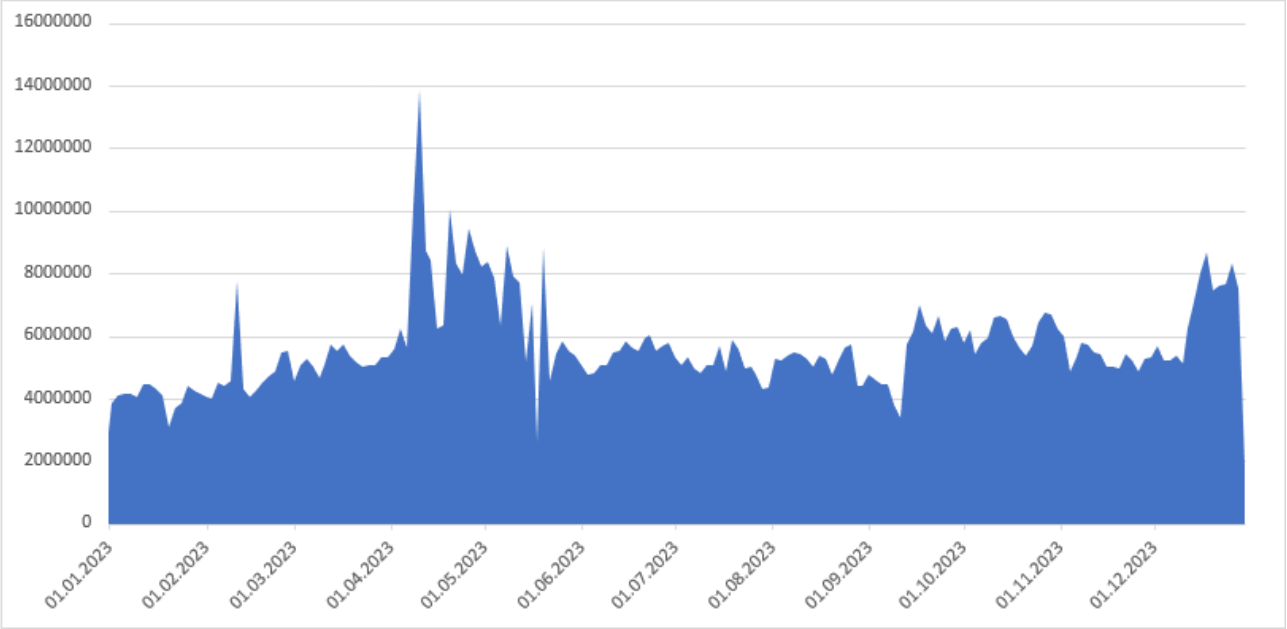
Bezpečnostní události v akademických sítích CESNET v roce 2023

Tato zpráva zahrnuje výsledky zpracování bezpečnostních událostí (incidentů) zaznamenaných v některých akademických sítích CESNET včetně sítě AV ČR v roce 2023 technickými prostředky bezpečnostního týmu Cesnet-Certs a archivovaných v databázovém systému Mentat.

Za roční období od 1. 1. 2023 do 31. 12. 2023 bylo v systému **Mentat** registrováno **104 184** záznamů s více než **1 030mil.** bezpečnostními událostmi zaznamenanými v sítích CESNET. Z toho více než **220mil.** událostí se týkalo sítě AV ČR a z nich přibližně **230tis.** byly v síti AV ČR iniciovány.

Bezpečnostní události v celé síti Cesnet



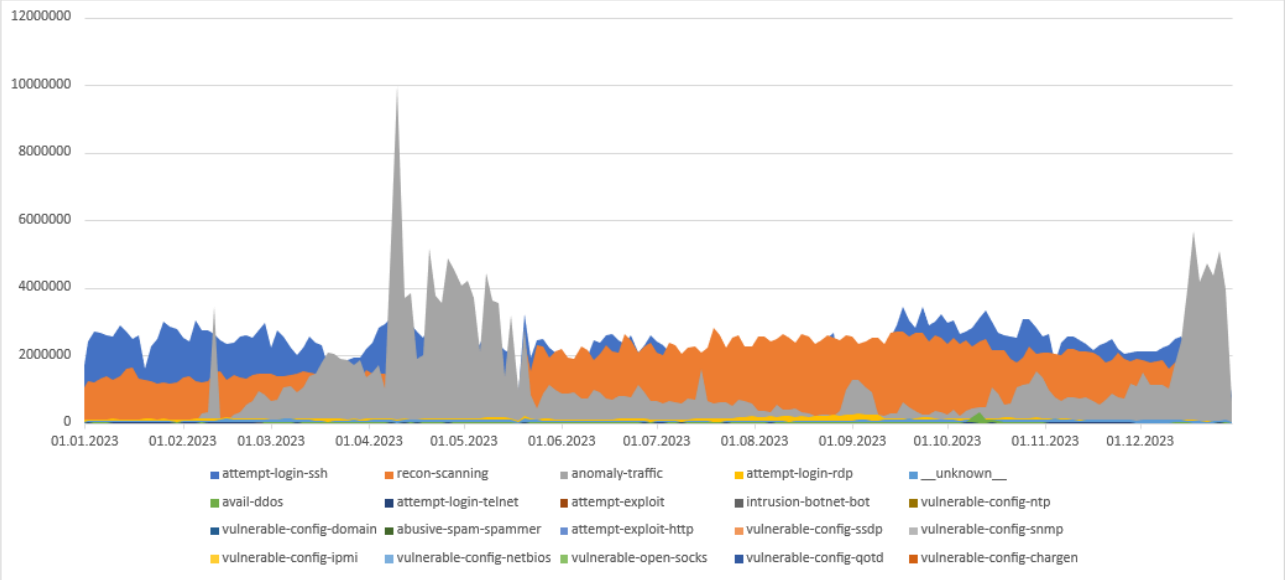
Obr. 1 Časová osa bezpečnostních událostí zaznamenaných v síti Cesnet od 1. 1. 2023 do 31. 12. 2023

Na obrázku (Obr.1) je zřejmý výrazný nárůst bezpečnostních událostí v dubnu 2023 s maximem ve dnech 8.4. a 10.4. Pokud by měla intenzita bezpečnostních událostí odrážet výskyt významných událostí ve veřejném životě, nabízí se Velikonoce, konkrétně Bílá sobota 8.3. a Velikonoční pondělí 10.3. Nelze vyloučit ani vazbu na probíhající boje na Ukrajině, zničení Kachovské přehrady s katastrofálními následky 6.4. 2023.

Podrobnější analýza ukázala, že z bezpečnostních událostí zaznamenaných v sítích CESNET byly nejčastější:

a) pokusy o neoprávněné připojení k cizímu počítači protokolem ssh (*Attempt-Login-ssh – 40,6 %)* a
b) skenování portů cizích počítačů (*Recon-Scanning - 33,4 %)*, které zřejmě poskytuje útočníkům základní informace o zranitelných a teoreticky dostupných systémech připojených do sítě Internet.
c) V průběhu měsíců březen až květen a na konci roku byl dále zaznamenán významný výskyt nestandardního, blíže neurčeného provozu (*Anomaly-trafic – 21,9 %*). Viz. Obr. 2.

Třídy bezpečnostních událostí v celé síti Cesnet

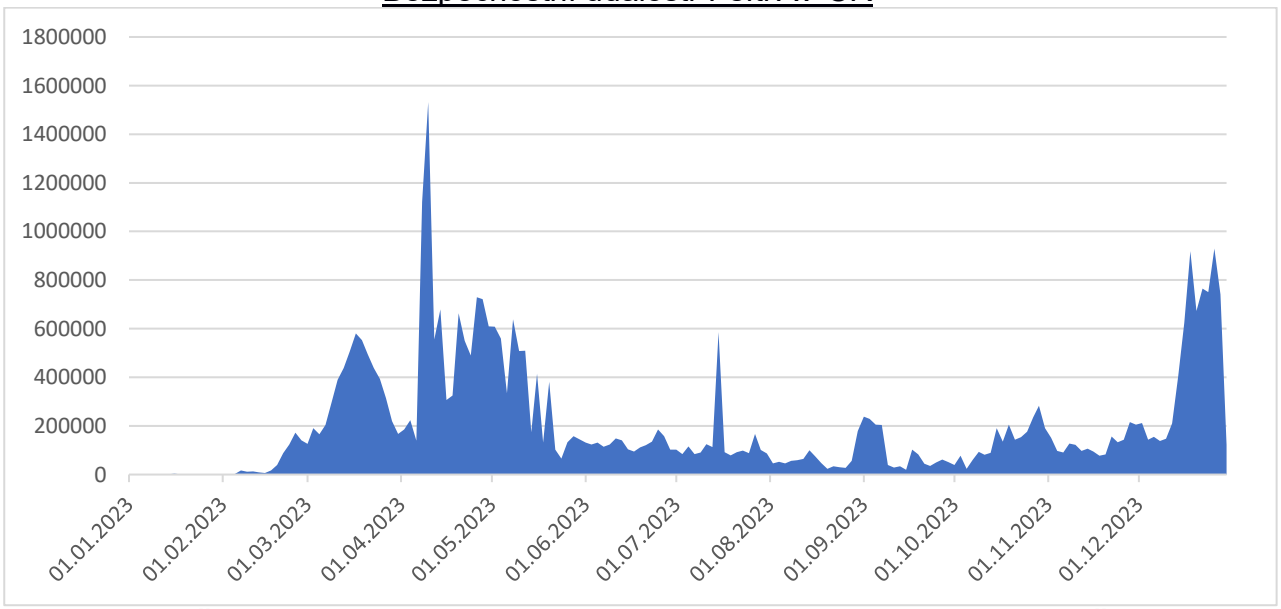


Obr. 2. Třídy bezpečnostních událostí zaznamenaných v síti Cesnet od 1. 1. 2023 do 31. 12. 2023

Bezpečnostní události v síti AV ČR

Síť AV ČR je součástí akademické sítě Cesnet. Informace o incidentech v síti AV ČR přijímá její bezpečnostní tým CAS-CSIRT na adrese abuse@cas.cz a následně je přeposílá správcům sítí pracovišť AV ČR, jichž se incident týká. Informace jsou zároveň ukládány do lokální databáze týmu pro jejích následnou analýzu.

Bezpečnostní události v síti AV ČR

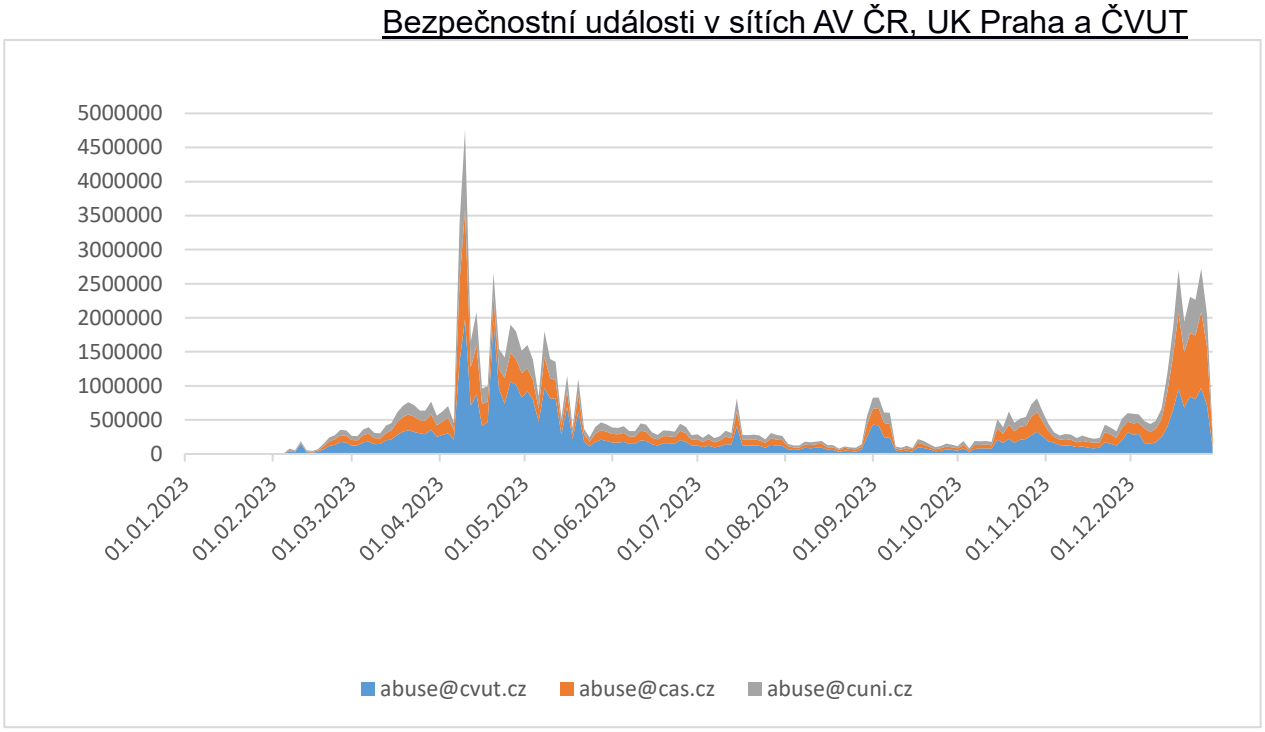


Obr. 3. Časová osa bezpečnostních událostí zaznamenaných v síti AV ČR od 1. 1. 2023 do 31. 12. 2023

Z porovnání časových os bezpečnostních událostí v síti Cesnet (Obr. 1) a AV ČR (Obr. 3) je patrné, že k výraznému zvýšení jejich výskytu došlo ve stejnou dobu v průběhu dubna a

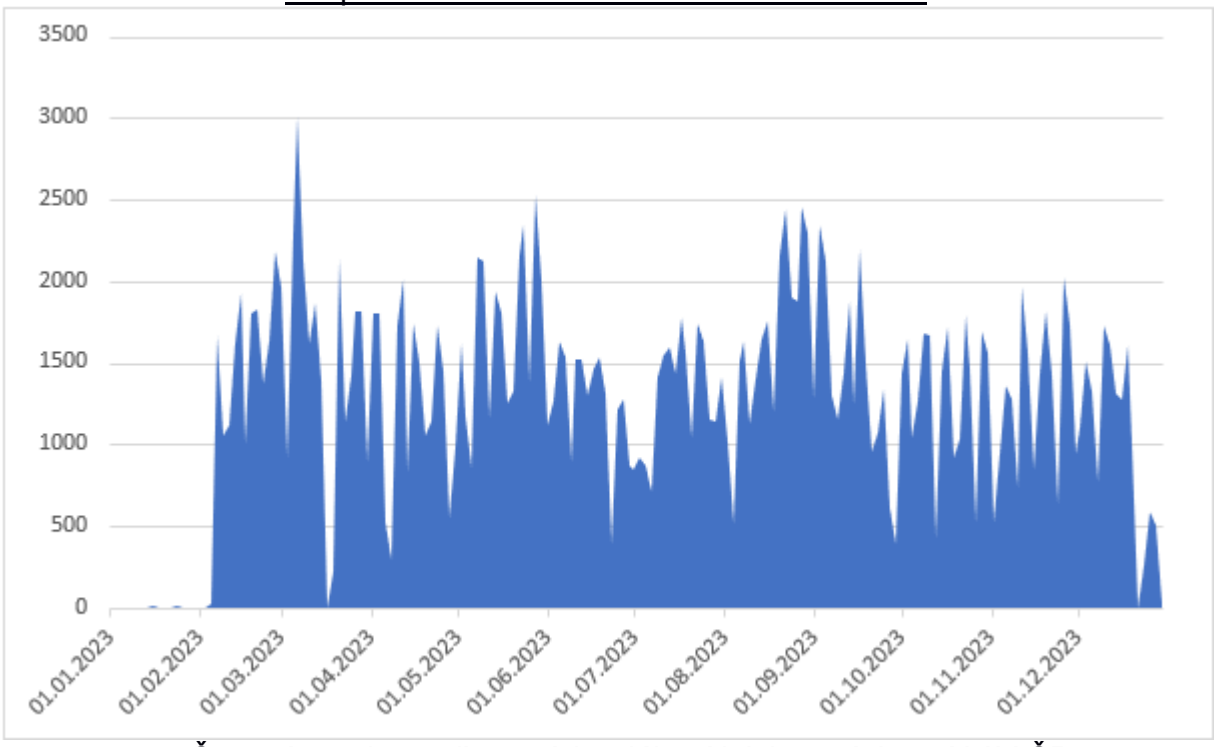
koncem roku 2023, pravděpodobně ze stejných příčin. Podíl počtu událostí v těchto termínech k počtu událostí v ostatních měsících roku je však v síti AV ČR výrazně vyšší. Z pohledu závislosti bezpečnostních událostí na vnějších vlivech je tedy síť AV ČR „citlivější“.

Podobný průběh bezpečnostních událostí v roce 2023 lze sledovat u všech tří největších akademických sítí: AV ČR, UK Praha a ČVUT. Podrobnější analýza naznačila, že převládajícími bezpečnostními událostmi zde byly různé typy testovacích provozů vyhodnocovaných jako Anomaly Traffic a Vulnerable.Config.



Obr. 4. Časová osa bezpečnostních událostí zaznamenaných v sítích AV ČR, UK Praha a ČVUT od 1. 1. 2023 do 31. 12. 2023

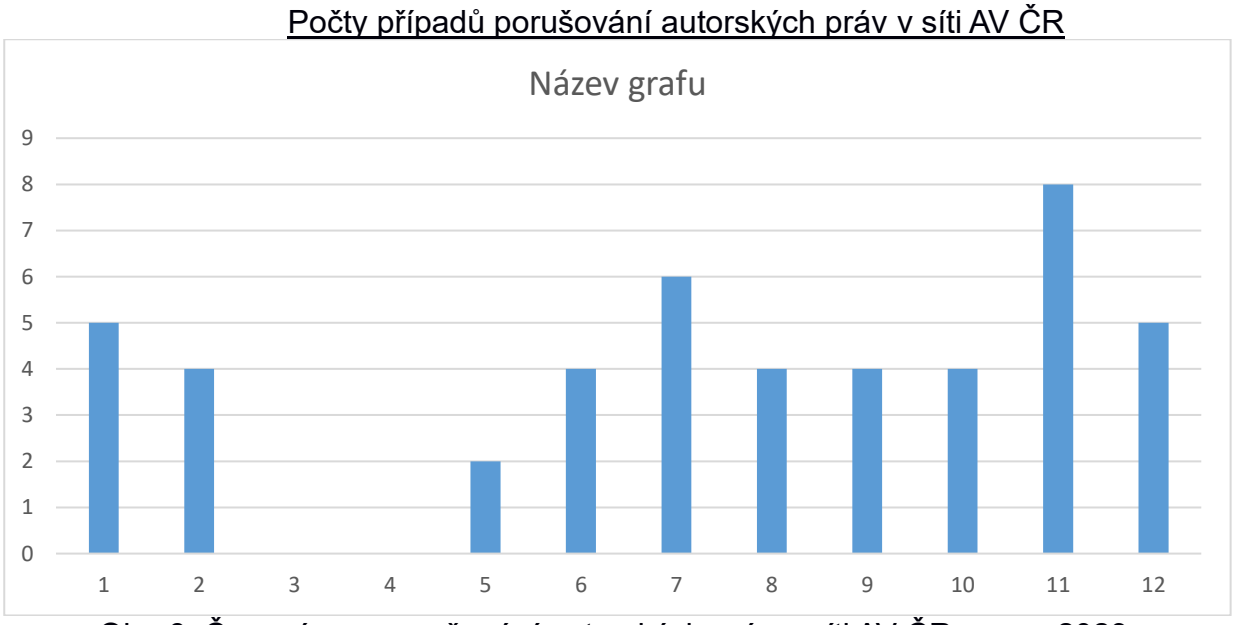
Dále jsme se zbývali i bezpečnostními událostmi, jejichž zdrojem jsou aktivní prvky sítě AV ČR. K bezpečnostním událostem v tomto případě řadíme i např. I chybnou konfiguraci počítače, jeho nedostatečně zabezpečené porty a v poslední době i porušování autorských práv neoprávněným šířením multimediálních dat prostřednictvím platformy Bittorent. Časovou osu těchto událostí zobrazuje Obr. 5.



Obr. 5. Časová osa bezpečnostních událostí iniciovaných v síti AV ČR od 1. 1. 2023 do 31. 12. 2023

V časové ose bezpečnostních událostí, mimo případy porušování autorských práv iniciovaných v síti AV ČR však lze sledovat jen jejich mírný záporný trend, který by teoreticky mohl být důsledkem účinných zásahů správců sítí.

Počty případů porušování autorských práv nejsou v síti AV ČR vysoké, pohybují se v počtech 40 – 50 případů ročně:



Obr. 6. Časová osa porušování autorských práv v síti AV ČR v roce 2023

K porušování autorských práv v síti Av ČR docházelo 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 autorském zákonu.

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 možnou korelaci těchto událostí s některými významnými událostmi v roce 2023.
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.

https://mentat.cesnet.cz
https://warden.cesnet.cz