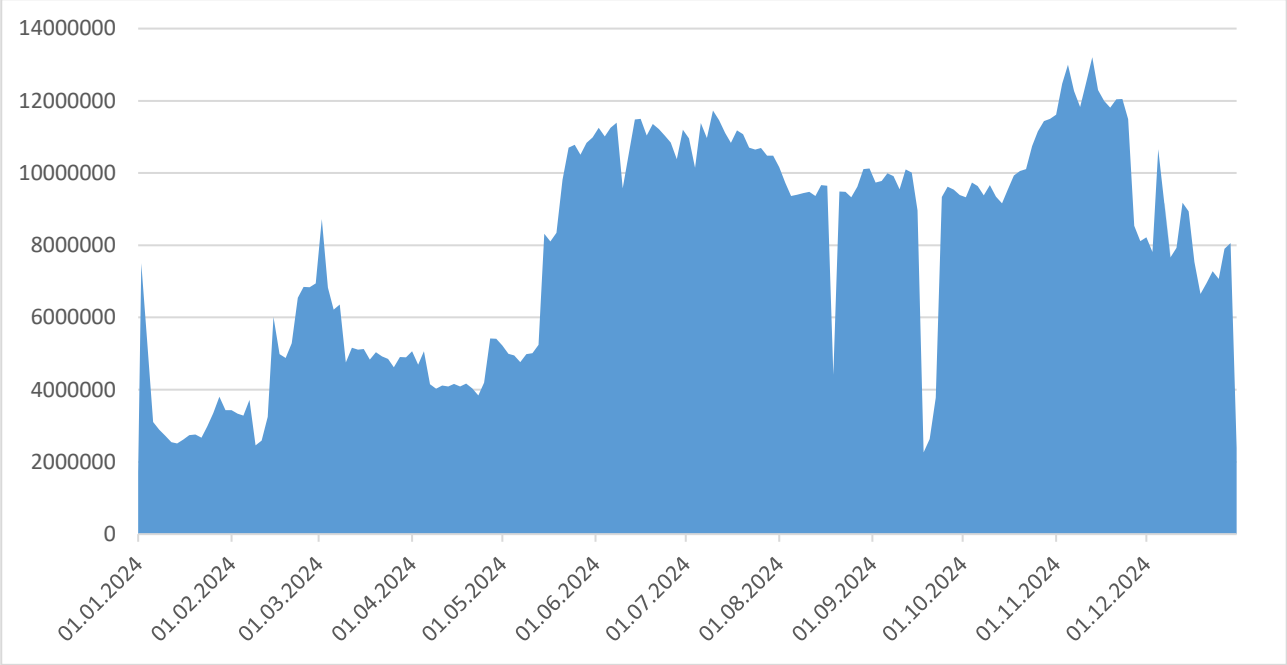
Bezpečnostní události v akademických sítích CESNET v roce 2024

Tato zpráva zahrnuje výsledky zpracování bezpečnostních událostí (incidentů) zaznamenaných v akademických sítích CESNET včetně sítě AV ČR v roce 2024 technickými prostředky bezpečnostního týmu Cesnet-Certs a archivovaných v databázovém systému Mentat.

Za roční období od 1. 1. 2024 do 31. 12. 2024 bylo v systému **Mentat** registrováno **104 523** záznamů s více než **1 447mil.** bezpečnostními událostmi zaznamenanými v sítích CESNET. Z toho více než **13 900tis.** událostí se týkalo sítí interních (AV ČR + VŠ) a z nich přibližně **500tis.** 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. 2024 do 31. 12. 2024

Na obrázku (Obr.1) je zřejmý výrazný nárůst bezpečnostních událostí na začátku druhého pololetí 2024 s maximem v listopadu 2024, konkrétně ve dnech 5.11. a 13.11. Pokud by tato maxima měla odrážet výskyt významných událostí ve veřejném životě, nabízí se vítězství Donalda Trumpa v prezidentských volbách (5.11.) a konference OSN v Baku o změně klimatu (11.11. – 22.11.).

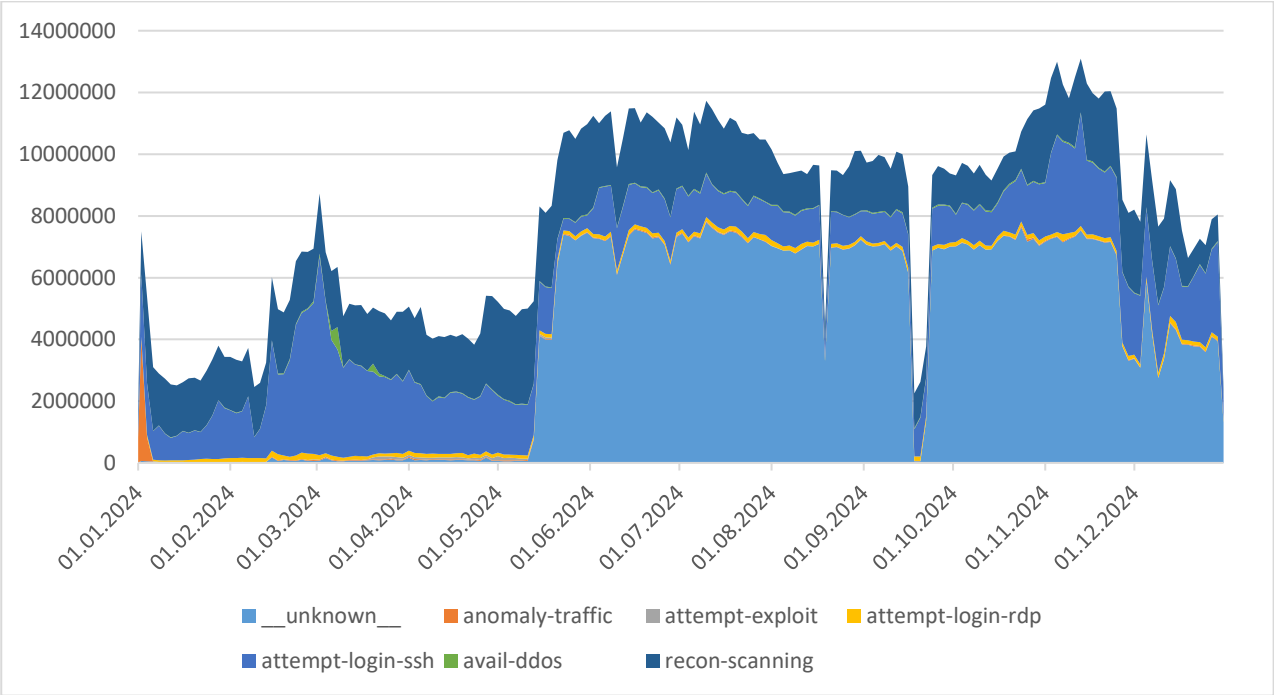
Podrobnější analýza událostí agregovaných do *tříd* ukázala, že z bezpečnostních událostí zaznamenaných v sítích CESNET v roce 2024 byly nejčastější:

a) skenování portů cizích počítačů (*Recon-Scanning - 24,14 %)*, poskytující útočníkům základní informace o zranitelných a teoreticky dostupných systémech připojených do sítě Internet
b) pokusy o neoprávněné připojení k cizímu počítači protokolem ssh (*Attempt-Login-ssh – 21,99 %)* a

c) pokusy o neoprávněné připojení k cizímu počítači protokolem rdp (*Attempt-Login-rdp – 1,59 %)*

V průběhu druhé poloviny roku 2024 byl pak zaznamenán významný výskyt nestandardního, blíže neurčeného provozu *(_unknown_)* odpovídajícího kategorii (*Intrusion.UserCompromise* nebo *Test – 50,99 %*). Viz. Obr. 2.

Třídy bezpečnostních událostí v celé síti Cesnet

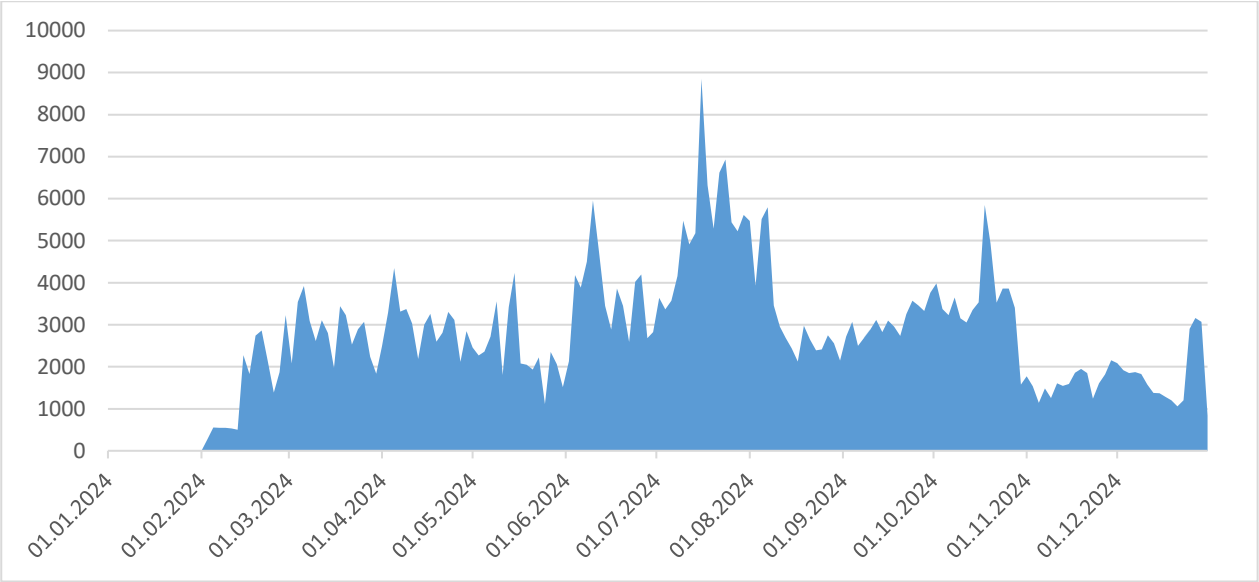


Obr. 2. Třídy bezpečnostních událostí zaznamenaných v síti Cesnet od 1. 1. 2024 do 31. 12. 2024

Bezpečnostní události v síti AV ČR

Síť AV ČR je součástí akademické sítě Cesnet. Jednotlivé ústavy AV ČR řeší bezpečnost svých sítí včetně eventuálního hlášení bezpečnostních incidentů Národnímu úřadu pro kybernetickou a informační bezpečnost samostatně, jejich společná evidence zatím neexistuje. Naproti tomu existuje společná evidence o bezpečnostních událostech se zdrojem v síti AV ČR. Informace o nich přijímá 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 se zdrojem v síti AV ČR



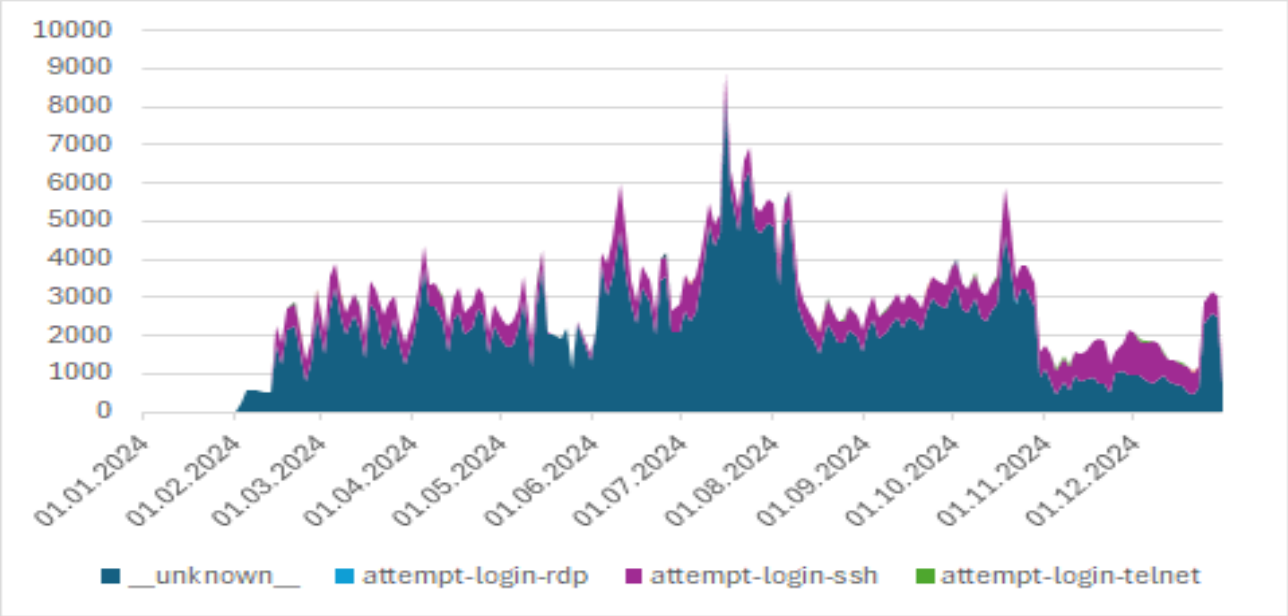
Obr. 3. Časová osa bezpečnostních událostí zaznamenaných v síti AV ČR od 1. 1. 2024 do 31. 12. 2024

Z porovnání časových os bezpečnostních událostí v síti Cesnet (Obr. 1) a AV ČR (Obr. 3) je patrné, že jejich průběh se zásadně liší. Zřejmě se tedy liší i mechanismy jejich vzniku.

Analýza událostí agregovaných do *tříd* ukázala, že ze všech bezpečnostních událostí se zdrojem v síti AV ČR v roce 2024 byly nejčastějšími pokusy o neoprávněné připojení k cizímu počítači (*Attempt-Login-ssh – 20,28 %),* nicméně téměř 80 % událostí nebylo možné jednoznačně ztotožnit s žádnou z definovaných tříd. Podrobnější analýza těchto "nezařazených" událostí však následně ukázala např. na možnou komunikací s botnetem (22,53%) a pravděpodobně šířený malware (10,58%) nebo phishingové zprávy (5,65%). Do kategorie "nezařazených" událostí patří i chybná konfigurace počítačů, např. nedostatečně zabezpečené porty (16,91%). (Obr. 4).

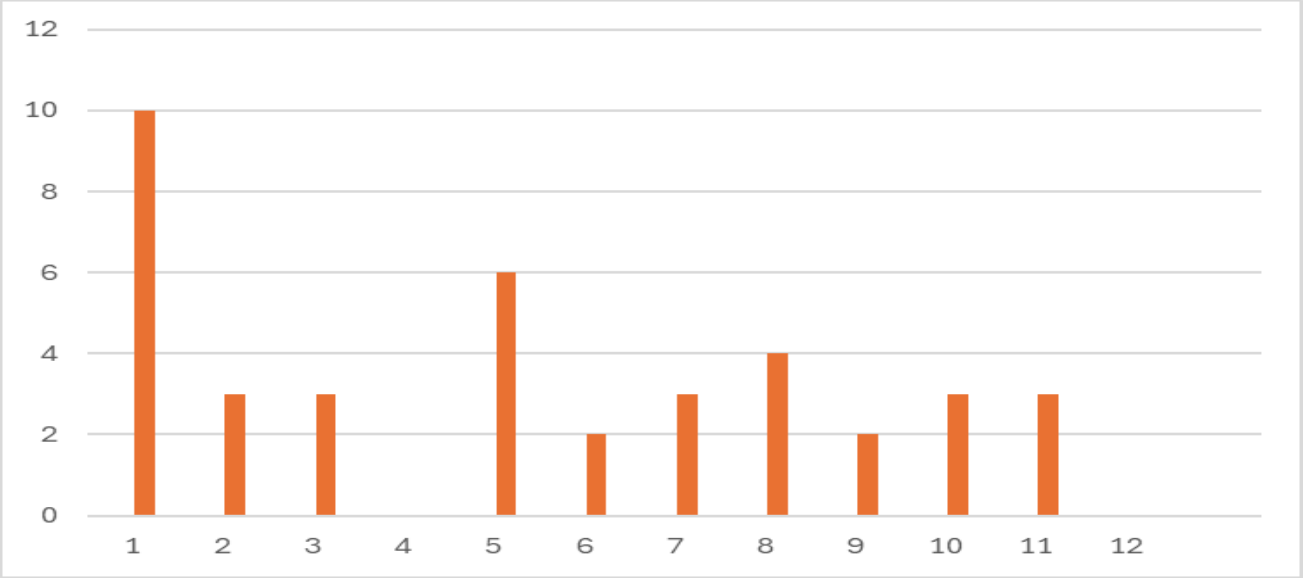
K bezpečnostním událostem se zdrojem v síti AV ČR jsme stejně jako v minulém roce zařadili i oznámené případy porušování autorských práv neoprávněným šířením multimediálních dat prostřednictvím platformy Bittorent. V průběhu celého roku bylo zaznamenáno 39 případů porušování autorských práv, což je prakticky stejný počet jako v minulém roce.
Časovou osu porušování autorských práv v síti AV ČR v roce 2024 ukazuje Obr.5.

Třídy bezpečnostních událostí v síti AV ČR



Obr. 4. Třídy bezpečnostních událostí zaznamenaných v síti AV ČR od 1. 1. 2024 do 31. 12. 2024

Porušování autorských práv v síti AV ČR



Obr. 5. Časová osa porušování autorských práv v síti AV ČR v roce 2024

V časové ose bezpečnostních událostí porušování autorských práv je nápadný jejich relativně vysoký počet v lednu 2024, který se však v dalších měsících patrně v důsledku účinných zásahů správců sítí již neopakoval.

Závěr

Cílem této studie byla analýza bezpečnostních událostí v akademických sítích, se zaměřením na síť AV ČR. Studie zároveň ukázala na možnou korelaci těchto událostí s některými významnými událostmi v roce 2024.

Výsledky studie naznačují, že ochrana proti stále sofistikovanějším kybernetickým útokům vyžaduje nejen stále dokonalejší firewally a podobná technická zařízení ale i značnou erudovanost jejich správců a samozřejmě i zodpovědné chování všech uživatelů.

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