NÁRODNÍ CENTRÁLA PROTI ORGANIZOVANÉMU ZLOČINU

služby kriminální policie a vyšetřování

odbor kybernetické kriminality

**POLICEJNÍ INTERNETOVÁ HOTLINE**

Statistický výstup za rok 2016

Obsah

[1 Kvantitativní analýza 3](#_Toc471739790)

[2 Kvalitativní analýza 5](#_Toc471739791)

[2.1 Rozdělení hlášení do oblastí možného protiprávního jednání 5](#_Toc471739792)

[2.2 Trendy 2016 6](#_Toc471739793)

[2.3 Vyřízení hlášení 6](#_Toc471739794)

[3 Závěrečné vyhodnocení 7](#_Toc471739795)

# 1 Kvantitativní analýza

V roce 2016 bylo prostřednictvím formuláře – pro hlášení závadového obsahu a aktivit v síti Internet, přijato **celkem 3 378 hlášení**. V porovnání s rokem 2015 se tedy jedná o mírný nárůst o 205 (cca 7 %) zaslaných hlášení. V následujícím grafickém zobrazení je znázorněna struktura předmětných hlášení, pro rok 2016.

**Rok 2016**

|  |  |
| --- | --- |
| **Relevantní** | **1 368** |
| **Nerelevantní** | 2 010 |

Jak je z tabulky a grafu patrné hlášení byla rozdělena do dvou základních kategorií. První jsou hlášení relevantní, u kterých je dán základ k dalšímu šetření a případnému využití v činnosti Policie ČR, případně dalších institucí. Kategorie nerelevantní pojímá veškerá hlášení, jenž svým obsahem nezakládají podezření z protiprávního jednání, jsou neaktuální nebo neobsahují žádné nové informace, které by z policejní činnosti již nebyly známy.

Z hlediska tohoto rozdělení je zřejmé, že **u cca 40%** přijatých je nezbytné komunikovat s ohlašovateli, případně provádět další šetření.

**Měsíční vývoj počtu hlášení**

Z porovnání nápadu hlášení mezi jednotlivými měsíci je patrné, že po tradičně nadprůměrných měsících leden a únor, došlo ke stabilizaci příjmu hlášení na počtu kolem 200. Nadprůměrný měsíc červen je způsoben opakovaně zasílaným hlášením jednoho ohlašovatele (500 ks) v průběhu měsíce května a června. *Viz grafické zobrazení níže*.

**Denní průměr oznámení za jednotlivé měsíce**

V roce 2016 byl zaznamenán obdobný průměrný denní počet přijatých hlášení v počtu cca **9 podání za den**. *Viz grafické zobrazení níže*.

# 2 Kvalitativní analýza

Relevantní přijatá hlášení jsou po svém administrativním zaevidování v systému ETŘ přidělena jednotlivým zpracovatelům. Ti provedou prvotní posouzení každého přijatého hlášení, z hlediska protiprávnosti a dále například akutnosti. V následující části jsou popsány oblasti, do kterých byla jednotlivá hlášení zařazena, nejčastěji se vyskytující protiprávní jednání, trendy roku 2016 a procentuální vyjádření způsobu vyřízení podání.

## 2.1 Rozdělení hlášení do oblastí možného protiprávního jednání

Relevantní hlášení, kterých bylo celkem 1 368, byla rozdělena celkem do 7 oblastí, které odkazují na jejich možné trestně-právní zařazení. V roce 2016 se nejpočetnější oblastí stala oblast podvodných jednání. Mezi tato řadíme veškerá podvodná jednání i přestupkového charakteru, která byla v daném roce prošetřována. *Viz graf níže*.

**Oblasti hlášení**

|  |  |
| --- | --- |
| **Podvodná jednání** | 532 |
| **Hacking** | 235 |
| **Mravnostní oblast** | 193 |
| **Ostatní** | 182 |
| **Extremismus** | 133 |
| **Násilí obecné** | 61 |
| **Autorská práva** | 32 |

Z grafického znázornění je patrné, že druhou nejvýznamnější skupinou byla jednání, související s infikací PC, DDoS útoky, ransomware a jiným obdobným jednáním. Vyjma extremistických projevů na internetu byla zaznamenána rovněž jednání spadající do oblasti násilí – vydírání, vyhrožování nebo kyberšikany. Oblast ostatní zahrnuje veškerá další jednání, která nespadají do těchto kategorií – občanskoprávní spory, poznatky o hledaných osobách, nebo například prodeji drog na internetu.

## 2.2 Trendy 2016

Rok 2016 se vyznačoval některými významnými trendy v problematice kybernetické kriminality, které se projevily rovněž v obsahu zaslaných hlášení hotline. Jednalo se o tyto trendy:

* *Ransomware útoky – uzamčení dat na PC a požadování výkupného např. v bitcoinech,*
* *virová nákaza šířená prostřednictvím příspěvků na sociálních sítích – Facebook aj.,*
* *využívání nedostatečně zabezpečených zařízení k DDoS útokům – internet věcí,*
* *phishingové e-maily či webové stránky s infikovaným obsahem – krádeže financí,*
* *podvodné inzeráty – fiktivní pronájmy bytů, prodeje vozidel,*
* *podvodné e-shopy,*
* *využívání relativní anonymity internetu k nenávistným projevům.*

Útoky na zařízení občanů, a to ať již mobilní nebo klasické PC, se stávají velmi častým jevem. Pachatelé se tímto způsobem snaží získat finanční prospěch, případně osobní data a další soukromé informace občanů.

## 2.3 Vyřízení hlášení

Po provedení předběžného šetření a případném vyhotovení zálohy závadového obsahu bylo hlášení buďto postoupeno jako poznatek místně a věcně příslušné součásti nebo uloženo ad acta k dalšímu služebnímu využití.

Jak zobrazuje graf výše, v roce 2016 bylo **cca 10% prošetřených hlášení,** vyhodnoceno jako způsobilé k dalšímu šetření jiným policejním orgánem.

# 3 Závěrečné vyhodnocení

V porovnání s předchozím rokem 2015 bylo v roce 2016 přijato prakticky totožné množství hlášení jako v roce 2015. Vyjma roku 2014 se tedy počet přijatých hlášení pohybuje stále ve stejných limitech, a to i co do počtu relevantních hlášení. **Od poloviny roku 2012 do konce roku 2016 bylo zaznamenáno celkově 18 580 hlášení HotLine**.

Problematickým aspektem služby policejní internetové HotLine zůstává fakt, že oproti původnímu záměru, kterým byl příjem zejména hlášení kyberkriminality, je služba občany využívána i k oznamování jiných protiprávních jednání, které nespadají do působnosti odboru kybernetické kriminality.