Klasifikace kybernetických útoků dle míry rozsahu a závažnosti – doplnění k bezpečnost- nímu auditu

# Anotace

I přesto, že má škola či jiná vzdělávací instituce vybudovanou bezpečnou ICT infrastrukturu a pravidelně provádí bezpečnostní audit, tak může dojít a často také dochází ke kybernetickým útokům. Ne každý útok je ale útokem na kybernetickou bezpečnost, a proto je důležité každou situaci individuálně posoudit a útok klasifikovat. K přesnější klasifikaci může posloužit následující tabulka závažnosti kybernetických útoků.

## A) Kritický incident

* Tyto incidenty obvykle znamenají velmi závažné narušení ICT infrastruktury a zasahují vysoký počet uživatelů.
* Jedná se o cílené kybernetické útoky na interní data.
* Zpřístupnění služeb dalším uživatelům.
* Cílené poškození reputace organizace.
* Značné finanční ztráty.

## B) Rozsáhlý incident

* Menší závažnost kybernetických útoků, avšak stále dochází k zasažení vysokého počtu uživatelů.
* Jedná se o neoprávněné přístupy a změny v systému.
* Napadání webových stránek.
* Běžné či distribuované odepření služby (DOS, DDOS)

## C) Drobný incident

* Tyto incidenty by měla automaticky detekovat a napravovat vnitřní bezpečnostní ICT infrastruktura.
* Jedná se například o monitorování sítě apod.

## D) Běžný incident

* Nepředstavují téměř žádné riziko pro bezpečnost ICT infrastruktury.
* Často se jedná o izolované spamy či drobná selhání hardwaru, například ztráta připojení k perifernímu zařízení apod.

Pakliže byla správně klasifikována závažnost útoku, musíme tentýž incident také podrobně identifikovat. K tomu je nutné zodpovědět následujících pět otázek:

**1. Kdo útok provedl?**

**2. Jaký je cíl útoku?**

**3. Kdy k útoku došlo?**

**4. Co bylo odcizeno, které informace byly ohroženy?**

**5. Jaký byl záměr útoku? (Finanční zisk, špionáž, výzva, zábava)**