**Formulář hlášení kybernetického bezpečnostního incidentu**

Identifikace ohlašovatele

* Dodavatel služby/produktu pro MERO CR, a.s.:
* Číslo smlouvy:
* Jméno a příjmení ohlašovatele:
* E-mail:
* Telefon:

Detaily kybernetického bezpečnostního incidentu / kybernetické bezpečnostní události:

Datum (YYMMDD) zjištění

Čas (HHMMSS 24hod. formát) zjištění

Datum (YYMMDD) ohlášení

Čas (HHMMSS 24hod. formát) ohlášení

Kategorie incidentů

□ Kategorie I – méně závažný kybernetický bezpečnostní incident

□ Kategorie II – závažný kybernetický bezpečnostní incident

□ Kategorie III – velmi závažný kybernetický bezpečnostní incident

Typ incidentu

□ Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb.

□ Kybernetický bezpečnostní incident způsobený škodlivým kódem.

□ Kybernetický bezpečnostní incident způsobený kompromitací technických opatření.

Současný stav zvládání kybernetického bezpečnostního incidentu

□ Probíhá analýza a šetření kybernetického incidentu

□ Dotčené funkce obnoveny

□ Neznámý

Popis incidentu

Rozsah škod, napadených systémů ve vztahu ke službám pro MERO ČR a.s.:

Již přijatá opatření:

Systémové detaily - cíl útoku (kompromitovaný systém):

Systémové detaily - zdroj útoku (je-li znám)

Zařízení / uživatel (Host / IP)

Port:

Protokol: