

Formulář hlášení kybernetického bezpečnostního incidentu

HLÁŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU	
MÍRA OCHRANY INFORMACE	
Úroveň ochrany	
	Osobní – seznam příjemců Omezená distribuce Neomezeno
KONTAKTNÍ ÚDAJE	
Orgán a osoba uvedená v § 3 písm. c) až e) zákona	
Email	
Telefon	
DETAILY INCIDENTU	
Datum a čas zjištění	
Časová zóna	
Kategorie incidentu	Kategorie III – velmi závažný kybernetický bezpečnostní incident Kategorie II – závažný kybernetický bezpečnostní incident Kategorie I – méně 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 překonáním technických opatření. Kybernetický bezpečnostní incident způsobený porušením organizačních opatření. Kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb. Ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem. Kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení integrity primárních aktiv.

	<p>Kybernetický bezpečnostní incident způsobující narušení dostupnosti primárních aktiv.</p> <p>Kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených shora.</p>
Současný stav zvládnutí kybernetického bezpečnostního incidentu	<p>Probíhá analýza a šetření kybernetického incidentu</p> <p>Kybernetický bezpečnostní incident je pod kontrolou</p> <p>Dotčené funkce obnoveny</p> <p>Neznámý</p>
Počet zasažených systémů (odhad)	
Odhad počtu dotčených uživatelů	
Popis incidentu	
SYSTÉMOVÉ DETAILY	
Host nebo IP	
Funkce hosta (DNS server, stanice atd.)	
Pokračování	<p>Iniciační oznámení CERTu</p> <p>Pokračování dříve oznámených</p>