Formulář hlášení kybernetického bezpečnostního incidentu

Míra ochrany informace *: Neomezeno (veřejné)
Omezená distribuce
Osobní - seznam příjemců

Kontaktní údaje

Instituce a osoba

Identifikátor ****:

E-mail *:

Telefon *:

Pokračování *: Iniciační oznámení / Pokračování dříve oznámeného incidentu **ID **:**

Detaily kybernetického bezpečnostního incidentu / kybernetické bezpečnostní události

Jedná se o hlášení: INCIDENTU / Události

Datum a čas zjištění *:	**YYYY**	**MM**	**DD**	**hh**	**: mm**	**Časová zóna*:**	**+- hh**
Datum a čas výskytu incidentu:	**YYYY**	**MM**	**DD**	**hh**	**: mm**	Časová zóna:	**+- hh**

Kategorie incidentu *: 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
- Kybernetický bezpečnostní incident způsobený škodlivým kódem
- Kybernetický bezpečnostní incident způsobený kompromitací technických opatření
- Kybernetický bezpečnostní incident způsobený porušením organizačních opatření
- Ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem
- Kybernetický bezpečnostní incident způsobující narušení dostupnosti primárních aktiv
- Kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených shora.

Upřesnění podle standardu ENISA/eCSIRT.net - "Incident Classification" ***:

- Abusive Content (např. spam, kyberšikana, nevhodný obsah)
- Malicious Code (např. virus, červ, trojský kůň, dialer, spyware)
- Information Gathering (např. skenování, sniffing, sociální inženýrství)
- Intrusion Attempts (např. zneužití zranitelnosti, kompromitace aktiva, "0-day" útok)
- Intrusions (např. kompromitace aplikace nebo uživatelského účtu)
- Availability (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)

- Information Security (např. neautorizovaný přístup nebo neautorizovaná změna informace, ...)
- Fraud (např. neoprávněné využití ICT - porušení licenčních práv, krádež identity aj.)
- ostatní

Současný stav zvládání kybernetického bezpečnostního incidentu *:

- Probíhá analýza a šetření kybernetického incident
- Kybernetický bezpečnostní incident je pod kontrolou
- Dotčené funkce obnoveny
- Neznámý

Počet zasažených systémů (odhad)*:

Odhad počtu dotčených uživatelů *:

Popis incidentu *:

Rozsah škod:

Jaká opatření již byla přijata?:

Systémové detaily - cíl útoku (kompromitovaný systém)

Host nebo IP *:

Funkce hosta *:

Port:

Protokol:

OS / jiný systém + verze:

Umístění systému v architektuře:

Systémové detaily - zdroj útoku (je-li znám)

Host / IP nebo jiné (zařízení/uživatel):

Port:

Protokol:

** Povinné pole*
*** Povinné pole v případě, že je vybrána volba "Pokračování dříve oznámeného incidentu", jedná se o ID dříve oznámeného incidentu / události, na které chcete navázat nové hlášení*
**** zdroj: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html*
***** Identifikátor zadávejte jen tehdy, pokud Vám byl sdělen ze strany KBMCSIRT*