**OBRAZEC ZA POROČANJE O KIBERNETSKEM INCIDENTU**

0. Osnovni podatki incidenta

|  |  |  |  |
| --- | --- | --- | --- |
| 0.1 | Referenčna številka incidenta  **(Določi odzivni center)** | Kliknite ali tapnite tukaj, če želite vnesti besedilo. | |
| 0.2 | Zadeva | Kliknite za zapis kratek opis incidenta. | |
| 1.5 | Poročilo |  | Prostovoljna priglasitev incidenta |
|  | Prvo poročilo o incidentu zavezanca |
|  | Vmesno poročilo o incidentu zavezanca |
|  | Končno poročilo o incidentu zavezanca |

1. Splošne informacije o poročevalcu

|  |  |  |  |
| --- | --- | --- | --- |
| 1.1 | Naziv subjekta, ki poroča | Kliknite za vpis naziva zavezanca. | |
| 1.2 | Sektor zavezanca | Izberite sektor. | |
| 1.3 | Kontaktni podatki za tehnična vprašanja | Ime priimek, naziv. | |
| Telefon. | |
| E-naslov. | |
| 1.4 | Kontaktna oseba zavezanca |  | Enaka kontaktni osebi za tehnična vprašanja. |
| Ime priimek, naziv. | |
| Telefon. | |
| E-naslov. | |

2. Začetne informacije o incidentu

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2.1 | Začetek / nastanek incidenta | | Izberi datum. | | Kliknite za vnos časa hh:mm. |
| Čas zaznave incidenta v sistemu | | Izberi datum. | | Kliknite za vnos časa hh:mm. |
| 2.2 | Opis incidenta | Kliknite za kratek opis zaznave in trenutne situacije vezane na kibernetski incident. | | | |
| 2.3 | Taksonomija | Klasifikacija incidenta (prva ocena). | | | |
| 2.5 | Ocena stopnje nevarnosti | Primarna ocena stopnje nevarnosti. | | Kliknite za dodaten opis kaj je potencialno ogroženo (sistem, informacije, storitev,…). | |
| 2.6 | Ocena možnega vpliva | Primarna ocena možnega vpliva. | | Kliknite za dodaten opis možnega vpliva incidenta (obseg in področje) ter potencialni mednarodni vpliv. | |
| 2.7 | Ocena stopnje incident | Glede na kriterije predlagana ocena stopnje kibernetskega incidenta. | | | |
| 2.8 | Opombe | Zapis vseh ostalih podatkov, ki bi lahko koristili v nadaljnjem upravljanju s kibernetskim incidentom. | | | |

3. Vmesno / končno poročanje

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3.1 | Poročilo | | | Vmesno | | | | | Končno | | |
| 3.2 | Čas zadnjega poročanja | | | izberite datum. | | | | | Kliknite za vnos časa hh:mm. | | |
| 3.3 | Trenutno stanje kibernetskega incidenta | | | V reševanju | | | | | Zaključen | | |
| 3.4 | Opis napake | Tehnični podatki o številu in vrsti sredstev, ki jih je prizadel kibernetski incident (naslovi IP, operacijski sistemi, aplikacije, strežniki in drugo). | | | | | | | | | |
| Okvara sistema | | |  | Okvara strežnika | | | |  | Socialni inženiring |
| Zloraba sistema | | |  | Zloraba strežnika | | | |  | Zloraba IP naslova |
| Nedelujoče aplikacije | | |  | Kraja podatkov | | | |  | Izsiljevalski virus |
|  | | |  |  | | | |  |  |
| Drugo: Kliknite za vnos besedila. | | | | | | | | | |
| 3.5 | Izvor incidenta | Vzrok kibernetskega incidenta, če je znan (odpiranje sumljive datoteke, povezovanje USB naprave, dostop do zlonamernega spletnega mesta in drugo). | | | | | | | | | |
| USB ključ | | |  | Spletno mesto | | | |  |  |
| Elektronsko sporočilo | | |  | Zlonamerne datoteke | | | |  |  |
| Vdor v sistem | | |  |  | | | |  |  |
|  | | |  |  | | | |  |  |
| Drugo: Kliknite za vnos besedila. | | | | | | | | | |
| 3.6 | Ogrožena storitev zavezanca |  | Bistvena storitev ZInfV | | | |  | Ostale storitve | | | |
| Katera bistvena storitev je ogrožena? Kliknite za vnos. | | | | | Katera storitev je ogrožena? Kliknite za vnos. | | | | |
| 3.7 | Taksonomija | Klasifikacija incidenta | | | | |  | | | | |
| 3.8 | Stopnja nevarnosti | Stopnja nevarnosti. | | | | | Kliknite za dodaten opis kaj je napadeno (sistem, informacije, storitev,…). | | | | |
| 3.9 | Vpliv incidenta | Vpliv kibernetskega incidenta. | | | | | Kliknite za dodaten opis vpliva incidenta (obseg in področje) ter potencialni mednarodni vpliv. | | | | |
| 3.10 | Stopnja incidenta | Glede na kriterije stopnje kibernetskega incidenta. | | | | | Stopnja po ZInfV  Izberite element. | | | | |
| 3.11 | Čezmejni vpliv incidenta | Ali ima kibernetski incident vpliv na katero drugo državo (katero, kakšen, kolikšen). | | | | | | | | | |
| DA NE | | Kliknite za vnos – če DA, na katero državo, kako in v kolikšni meri? | | | | | | | |
| 3.12 | Akcijski načrt in protiukrepi | Kateri ukrepi so bili sprejeti za ustavitev širjenja in nadaljevanja kibernetskega incidenta ter kateri ukrepi za odpravo kibernetskega incidenta. Kateri protiukrepi in ukrepi so še načrtovani v nadaljevanju reševanja kibernetskega incidenta. | | | | | | | | | |
| Že sprejeti ukrepi: Kliknite za vnos besedila. | | | | | | | | | |
| Načrtovani ukrepi: Kliknite za vnos besedila | | | | | | | | | |
| 3.13 | Povzročena škoda | Kliknite za vnos ocene materialne škode ali škode povzročene imenu zavezanca. | | | | | | | | | |
| 3.14 | Potrebe za odpravo posledic | Tehnično osebje in tehnična sredstva, ki so potrebna za odpravo incidenta in jih zavezanec neposredno nima na razpolago. Predvideno število dni za odpravo kibernetskega incidenta. | | | | | | | | | |
| 3.15 | Časovni okvir odprave posledic | Ocena koliko časa po zaključenem incidentu bo zavezanec potreboval, da bo odpravil posledice incidenta ter stanje (sistemov, omrežij, storitev,…) povrnil nazaj v običajno, kot je bilo pred kibernetskim incidentom. | | | | | | | | | |
| 3.16 | Opombe | Kliknite za zapis vseh ostalih podatkov, ki niso zajeti v zgornjih točkah. | | | | | | | | | |
| 3.17 | Priloge | Seznam priloženih dokumentov, ki bodo pomagali poznati vzrok težave ali njeno razrešitev (posnetki zaslona, datoteke z informacijami, elektronska pošta, logbooki in drugo). | | | | | | | | | |
| Kliknite za vnos besedila. | | | | | | | | | |
|  | | | | | | | | | |

**NAVODILA ZA IZPOLNJEVANJE**

1. Zavezanec obvesti nemudoma odzivni center o kibernetskem incidentu v njegovih sistemih ali omrežjih.
2. Pri prvem poročanju obvezno izpolni:
   1. 0. META PODATKE,
   2. 1. SPLOŠNE PODATKE O POROČEVALCU
   3. 2. ZAČETNE PODATKE O INCIDENTU (podatki, ki so na voljo)
3. Pri vmesnem poročanju izpolni:
   1. Ohrani 0. META PODATKE in 1. SPLOŠNE PODATKE O POROČEVALCU
   2. 3. Vmesno / končno poročanje (podatki, ki so na voljo)
4. Pri končnem poročanju izpolni:
   1. Ohrani 0. META PODATKE in 1. SPLOŠNE PODATKE O POROČEVALCU
   2. 3. Vmesno / končno poročanje
5. Odzivni center lahko po potrebi med upravljanjem s kibernetskim incidentom komunicira z zavezancem za dodatna pojasnila in izpolnjevanje delov obrazca.