Картка інформування про кіберінцидент/кібератаку

|  |
| --- |
| ***Примітка:***1. *Для позначення потрібних варіантів підкреслити (обвести, виділити кольором) обраний варіант.*
2. *Намагатися вказати якомога більше інформації, заповнивши відповідні поля.*
 |
| **TLP** |
| RED | AMBER | AMBER + STRICT | GREEN | CLEAR |
| Дата та час виявлення кіберінциденту/кібератаки: | \_\_\_.\_\_\_.\_\_\_\_ \_\_\_:\_\_\_:\_\_\_ GMT \_\_\_\_\_ |
| **Заявник** |
| ПІБ: |  | Електронна адреса: |  |
| Посада: |  | Номер телефону: |  |
| Суб’єктзабезпечення кібербезпеки: | Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського” |
| **Джерело виявлення кіберінциденту/кібератаки** |
| Адміністратор | Користувач | Антивірусне ПЗ | EDR |
| IDS/IPS | Інше(вказати):  |
| **Запропонована категорія (рівень) критичності кіберінцидент/кібератаки** |
| 0, некритичний (білий) | 1, низький (зелений) |
| 2, середній (жовтий) | 3, високий (помаранчевий) |
| 4, критичний (червоний) | 5, надзвичайний (чорний) |
| Не вдалося визначити |
| **Отримана інформація** |
|  |
| **Постраждалий суб’єкт забезпечення кібербезпеки** |
| Юридична назва: |  |
| Адреса: |  |
| Електронна адреса: |  | Номер телефону: |  |
| Контактна особа 1 |
| ПІБ: |  | Електронна адреса: |  |
| Посада: |  | Номер телефону: |  |
| Контактна особа 2 |
| ПІБ: |  | Електронна адреса: |  |
| Посада: |  | Номер телефону: |  |
| **Сектор (галузь) атакованого об’єкта** |
| Сектор безпеки і оборони | Органи державноївлади | Органи місцевого самоврядування | Енергетичний сектор |
| Сфера електронних комунікаційнихпослуг | ІТ сектор | Транспортна галузь | Фінансовий сектор |
| Підприємства таорганізації відповідної форми власності | Засоби масової інформації | Інші критичні організації | Інше (вказати):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Доменна зона** |
| UAGOVУкраїнський державний | UACOMУкраїнський недержавний | FGOVЗакордонний державний | FCOMЗакордонний недержавний |
| **Відношення України до кіберінциденту/кібератаки** |
| Україна – об’єкт атаки | Україна –джерело атаки | Україна – елемент механізму атаки | не стосується території України |
| Інше(вказати): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Категорія та тип кіберінциденту (відповідно до Переліку категорій та типів кіберінцидентів)** |
| *Код* | *Категорія кіберінциденту* | *Код* | *Тип кіберінциденту* |
| 01 | Шкідливий (образливий) вміст (Abusive content) | 01 | Спам |
| 02 | Шкідливий програмний код (Malicious Code) | 01 | Зараження шкідливим програмним забезпеченням (ШПЗ) |
| 02 | Розповсюдження ШПЗ |
| 03 | Командно-контрольний центр (С2) |
| 04 | Шкідливе підключення |
| 03 | Збір інформації зловмисником (Information Gathering) | 01 | Сканування |
| 02 | Сніфінг |
| 03 | Фішинг |
| 04 | Спроби втручання (Intrusion Attempts) | 01 | Спроба експлуатації вразливості |
| 02 | Спроби авторизації/входу в систему |
| 05 | Втручання (Intrusion) | 01 | Компрометація облікового запису |
| 02 | Компрометація системи |
| 06 | Порушення доступності (Availability) | 01 | Атака на відмову в обслуговуванні |
| 02 | Саботаж/шкідливі дії |
| 03 | Збій |
| 07 | Порушення властивостей інформації (Information Content Security) | 01 | Несанкціонований доступ до інформації |
| 02 | Несанкціонована модифікація |
| 08 | Шахрайство (Fraud) | 01 | Шахрайський сайт |
| 09 | Відома вразливість (Vulnerable) | 01 | Вразливість |
| 02 | Некоректна конфігурація |
| 10 | Інше (Other) | 01 | Невизначений інцидент |
| Дата та час початку кіберінциденту/кібератаки: | \_\_\_.\_\_\_.\_\_\_\_ \_\_\_:\_\_\_:\_\_\_ GMT \_\_\_\_\_ |
| **Чи пов’язаний цей (ця) кіберінцидент/кібератака з попередніми?** |
| ТАК | НІ | ID пов’язаного кіберінциденту/кі- бератаки: \_\_\_\_\_\_\_\_\_ | Невідомо |
| **Короткий опис кіберінциденту/кібератаки** |
|  |
| **Вплив на функціонування систем/мереж, сервіси (послуги)** |
| Немає впливу взагалі | Немає впливу на сервіси (послуги) |
| Мінімальний вплив на некритичні сервіси (послуги) | Мінімальний вплив на критичні сервіси (послуги) |
| Значний вплив на некритичні сервіси (послуги) | Значний вплив на некритичні сервіси (послуги) |
| Втрата доступності некритичних сервісів (послуг) | Втрата доступності критичних сервісів (послуг) |
| **Кількість скомпрометованих систем/мереж (ЕОМ)** |
| 1-10 | 10-50 | Інше (вказати): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Невідомо |
| **Тип скомпрометованої системи/мережі за функціоналом** |
| Робочі станції | Сервер(и) додатків | Сервер(и) баз даних | Вебсервер(и) |
| Сервери доменних імен | Поштовий сервер | Брандмауер(и) | Мережеве обладнання |
| Інше(вказати): |
| **Об’єкт кібератаки** |
| Тип (модель): |  |
| Ім'я: |  |
| Операційна система: |  |
| Дата встановлення ОС: |  |
| Часова зона: |  |
| Мережеві налаштування: |  |
| Облікові записи: |  |
| CVE: | CVE- - | CVE- - | CVE- - |
| Висновок: |
| Тип (модель): |  |
| Ім'я: |  |
| Операційна система: |  |
| Дата встановлення ОС: |  |
| Часова зона: |  |
| Мережеві налаштування: |  |
| Облікові записи: |  |
| CVE: | CVE- - | CVE- - | CVE- - |
| Висновок: |
| Тип (модель): |  |
| Ім'я: |  |
| Операційна система: |  |
| Дата встановлення ОС: |  |
| Часова зона: |  |
| Мережеві налаштування: |  |
| Облікові записи: |  |
| CVE: | CVE- - | CVE- - | CVE- - |
| Висновок: |
| **Чи вирішено****кіберінцидент/кібератаку?** | **Чи потрібна допомога CERT-UA?** |
| Так | Ні | Так | Ні |
| **Чи повідомлялося про кіберінцидент/кібератаку іншим основним суб’єктам забезпечення кібербезпеки? Яким саме?** |
| Так | Ні |
| Служба безпеки України | Міністерство оборониУкраїни та Генеральний штаб Збройних Сил України | Розвідувальні органи |
| Національний банк України | Національна поліція України | Національнийкоординаційний центр кібербезпеки при РНБО України |
| Департамент кіберполіції Національної поліції України | Коментар: |
| **Чи залучалися сторонні організації до вирішення кіберінциденту/кібератаки?** |
| Так | Ні |
| Інший CERT, CSIRT, SOC | Антивірусні компанії | Обслуговуюча компанія, інтегратор,представник вендора | Інше (вказати): |
| Коментар: |
| **Результат впливу** |
| Витік даних | Злам (компрометація) системи | Втрата функціональності систем/сервісів | Інше (вказати): |
| **Від потенційного впливу кіберінциденту/кібератаки на державному рівні під загрозою** |
| Національна безпека | Сталість економіки | Національний імідж | Функціонування Уряду |
| Безпека персональних даних громадян | Інше:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Індикатори компрометації** |
| *Мережеві:* |
| IP/домен/URL/User Agent | Коментар |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| *Хостові:* |
| Шлях/команда/сервіс/заплановане завдання/гілка реєстру | Коментар |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| *Файлові:* |
| Хешсума файлу | Назва файлу | Коментар |
| MD5(приклад): [хешсума] |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **Перелік отриманих даних** |
| Хешсума файлу | Назва файлу | Коментар |
| MD5(приклад): [хешсума] |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |