

План дій у випадку виявлення кіберзагрози

1. Негайні дії на місці інциденту

1.1. Ідентифікація кіберзагрози:

- Визначити тип загрози (вірус, спроба несанкціонованого доступу, підозрілий трафік, вразливість в системі тощо).
- Якщо можливо, зробити скріншоти або зберегти журнали подій, що підтверджують інцидент.

1.2. Ізоляція ураженого компонента:

- Відключіть від мережі підозрілий пристрій або сервер, щоб мінімізувати поширення загрози.
- Заблокуйте доступ до зовнішніх ресурсів, які можуть бути джерелом атаки.

1.3. Фіксація даних:

- Зафіксуйте час, IP-адреси, порти, шляхи доступу, з якими пов'язана підозра.
- Збережіть відповідні файли, журнали та підозрілі дані для подальшого аналізу.

2. Інформування ключових сторін

2.1. Сповіщення внутрішньої команди:

- Повідомте керівництво та спеціалістів кібербезпеки про загрозу.
- Забезпечте передачу всіх зібраних доказів і опису інциденту.

2.2. Інформування CERT-UA:

- Відправте офіційне повідомлення до CERT-UA за допомогою електронної пошти або через їхній веб-сервіс:
 - Опис інциденту.
 - Характер загрози.
 - Додайте файли із зібраними даними (журнали, зразки шкідливого ПЗ тощо).
- Контакти CERT-UA доступні на їхньому офіційному веб сайті (також в кінці цієї інструкції).

3. Сповіщення MISP-UA:

- Передайте технічні дані загрози (IoC — Indicators of Compromise) через платформу MISP-UA.
- Додайте відповідні теги та пояснення для точної класифікації.

4. Спільнота кіберпідхоти:

- Інформуйте спільноту через визначені безпечні канали (Google Chat), зберігаючи конфіденційність деталей організації.

5. Дії щодо нейтралізації загрози

5.1. Аналіз загрози:

- Проаналізуйте самостійно або з допомогою експертів кібербезпеки, або з допомогою CERT-UA та MISP-UA.
- Використовуйте спеціалізовані інструменти (наприклад, Wireshark, Splunk, інші IDS/IPS).

5.2.Знешкодження:

- Застосуйте оновлення безпеки, патчі або видаліть шкідливі файли.
- Перевірте резервні копії та відновіть систему з безпечного стану, якщо необхідно.

6. Запобіжні заходи для майбутнього

6.1.Оновлення політик безпеки:

- Перегляньте існуючі правила доступу, моніторингу та обробки інцидентів.
- Впровадьте багаторівневий захист.

6.2.Проведення навчань:

- Проведіть тренінги для співробітників з розпізнавання кіберзагроз.
- Симулюйте кіберінциденти для покращення реагування.

6.3.Моніторинг і аудити:

- Впровадьте регулярний аналіз мережевого трафіку та вразливостей.
- Використовуйте SIEM-системи для цілодобового моніторингу.

7. Документування інциденту

7.1.Підготуйте детальний звіт, що включає:

- Опис інциденту та вжитих дій.
- Висновки щодо впливу на систему.
- Рекомендації для запобігання повторним атакам.

7.2. Звіт належить довести до відома керівництву управління, спеціалістам по кіберзахисту та **CERT-UA**

7.3. Картка інформування про кіберінцидент/кібератаку згідно Наказу №570 Адміністрації державної служби спеціального зв'язку та захисту інформації України, Додаток 6 до Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій в кіберпросторі (пункт 6 розділу III) складається головним спеціалістом відділу кіберзахисту.

8. Контакти для екстреного реагування

- Головний спеціаліст кіберзахисту Управління: +380634917783

CERT-UA: cert.gov.ua

incidents@cert.gov.ua

Пн - Чт: 8:00 - 17:00, Пт: 8:00 - 15:45:

+38 (044) 281-88-25

+38 (044) 281-88-05

Вихідні та святкові дні (цілодобово):

+38 (044) 281-88-01

- MISP-UA: через кабінет управління або support@dis.gov.ua

- Спільнота кіберпіхоти: Google Chat

Ретельне виконання цього плану допоможе знизити ризики та мінімізувати збитки від кіберзагроз.