**План реагування на інциденти та загрози для телекомунікаційної компанії NauStilus**

**Вступ**

У сучасному цифровому середовищі телекомунікаційні компанії відіграють ключову роль у забезпеченні критичної інфраструктури, доступу до інформації та підтримці національної кіберстійкості. З огляду на зростання кількості кіберінцидентів, зокрема витоків даних, DDoS - атак, шкідливого програмного забезпечення та фізичних загроз, питання побудови ефективної системи реагування на інциденти набуває особливої актуальності.

Компанія NauStilus, як умовний приклад телекомунікаційного оператора, розглядається в цьому документі як суб’єкт, що прагне впровадити комплексний підхід до управління кіберзагрозами. План реагування, представлений нижче, є результатом моделювання сценаріїв, адаптованих до українського законодавства, міжнародних стандартів та галузевих практик.

Документ базується на принципах, викладених у NIST SP 800-61 (Computer Security Incident Handling Guide), ISO/IEC 27035 (Information Security Incident Management), а також враховує вимоги GDPR та Закону України «Про захист персональних даних». Він охоплює повний життєвий цикл інциденту - від виявлення до відновлення, включаючи класифікацію, комунікацію, технічне реагування, юридичну оцінку та постінцидентний аналіз.

Увагу приділено ролям учасників процесу реагування: менеджеру з інцидентів, аналітику SOC, ІТ-персоналу, юридичному представнику, PR-фахівцю, Red Team та фізичній охороні. Для кожної ролі визначено функціональні обов’язки, з урахуванням специфіки телеком - інфраструктури та потенційних загроз.

У документі розроблено сценарії реагування на витік персональних даних (з критичною та некритичною інформацією), DDoS-атаки різного рівня складності, а також виявлення шкідливого ПЗ, включаючи варіант скритого реагування з метою деанонімізації зловмисника.

Важливою складовою плану є встановлення SLA - часових рамок для виявлення, реагування, усунення та відновлення системи. Це дозволяє забезпечити контрольовану швидкість дій та відповідність очікуванням внутрішніх і зовнішніх стейкхолдерів.

Інструменти виявлення інцидентів включають SIEM-системи, IDS/IPS, EDR-рішення, honeypots, threat intelligence та симуляції Red Team. Їх використання дозволяє забезпечити про активне виявлення аномалій та швидке реагування.

Класифікація інцидентів за рівнем серйозності (високий, середній, низький) базується на оцінці впливу на репутацію, юридичні наслідки, фінансові втрати та порушення законодавства. Це дозволяє адаптувати реагування до конкретного контексту.

Комунікаційний план охоплює внутрішні та зовнішні канали, визначає типи повідомлень (тривожні, регулярні, фінальні), аудиторії (співробітники, клієнти, медіа, регулятори) та шаблони для різних сценаріїв. Додано скрите реагування, яке передбачає обмежене інформування до завершення розслідування.

Процедури відновлення включають роботу з резервними копіями, заміну обладнання або ПЗ, перевірку систем після відновлення та реагування на великі інциденти. Для кожного етапу визначено конкретні дії, що забезпечують цілісність даних та стабільність сервісів.

Оцінка, стримування та розслідування є завершальним етапом реагування. Вона включає форензичний аналіз, поведінкову деанонімізацію, підготовку доказової бази та юридичне реагування. У випадках шпигунства або фізичного проникнення застосовується скрите реагування з метою фіксації дій зловмисника.

Окремий розділ присвячено фізичним загрозам: потраплянню сторонніх осіб до серверних, підпалу або фізичному знищенню обладнання, виявленню шпигунського обладнання. Для кожного сценарію визначено дії, які мають бути здійснені без розголосу, з участю фізичної охорони та SOC.

Цей документ спроба створити не лише технічний, але й стратегічний інструмент, що дозволяє компанії NauStilus забезпечити кіберстійкість, відповідність нормативним вимогам та довіру клієнтів.

У процесі розробки я намагався врахувати кейси з відкритих джерел, конспекту, рекомендації Microsoft щодо реагування на інциденти, а також принципи безперервного вдосконалення.

Можливо представлений план може бути прикладом для побудови ефективної системи реагування на інциденти, який поєднує технічну, нормативну, та організаційну сторони.

Як варіант у майбутньому він може бути доповнений механізмами автоматизації, інтеграцією з SOC-платформами та сценаріями реагування на атаки з використанням штучного інтелекту.

1. **Ідентифікація ролей та відповідальностей**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Опис функцій** | **Основні обов’язки** |
| **Менеджер з інцидентів** | Координує всі етапи реагування, приймає рішення щодо ескалації, ізоляції, відновлення. Взаємодіє з усіма командами та відповідає за фінальний звіт | Призначення відповідальних  Контроль SLA  Ескалація  Затвердження плану  Комунікація з керівництвом  Звітність |
| **Аналітик безпеки (SOC)** | Виявляє, класифікує та аналізує інциденти. Працює з SIEM, IDS/IPS, проводить кореляцію подій | Моніторинг  Аналіз логів  Класифікація  Форензика  Звітність  Взаємодія з Red Team |
| **ІТ-персонал** | Відповідає за технічну ізоляцію, відновлення, патчинг, тестування. | Ізоляція  Відновлення  Патчинг  Заміна обладнання  Тестування  Документування |
| **Юридичний представник** | Оцінює правові наслідки, готує документи, взаємодіє з регуляторами. | Аналіз відповідності  Повідомлення регуляторів  Юридичні висновки  Підтримка розслідування  Захист інтересів |
| **PR-фахівець** | Забезпечує контрольовану комунікацію з громадськістю та клієнтами | Шаблони повідомлень  Взаємодія з медіа  Комунікація з клієнтами  Внутрішнє інформування  Репутаційний контроль |
| **Red Team** | Проводить симуляції атак, бере участь у прихованому реагуванні. | Симуляції  Виявлення бекдорів  Деанонімізація  Підготовка доказів  Взаємодія з SOC |
| **Фізична охорона** | Контролює фізичний доступ, реагує на фізичні загрози. | Відеоспостереження  Контроль доступу  Виявлення сторонніх  Реагування  Збереження доказів |

1. **Процедури реагування на інциденти**

*Витік персональних даних*

|  |  |
| --- | --- |
| **Тип** | **Дії** |
| **Без критичної інформації** | Ізоляція системи- Повідомлення менеджеру - Аналіз логів - Оцінка обсягу витоку- Відновлення доступу |
| **З критичною інформацією** | Повна ізоляція - Форензика - Повідомлення регуляторів - Комунікація - Відновлення (Оновлення політик) |

*DDOS-атака*

|  |  |
| --- | --- |
| **Тип** | **Дії** |
| **DoS** | Виявлення - Фільтрація трафіку- Відновлення доступу |
| **DDoS** | WAF/CDN - Взаємодія з провайдером - Моніторинг |
| **Botnet** | Виявлення - Блокування ІР - Аналіз джерел |
| **Botnet + проникнення** | Ізоляція - Форензика - Скритий моніторинг - Деанонімізація - Відновлення |

*Шкідливе ПЗ*

|  |  |
| --- | --- |
| **Тип** | **Дії** |
| Стандартне | Виявлення - Видалення - Патчинг - Відновлення |
| Скрите реагування | Виявлення(бекдору) - Моніторинг - Логування дій зловмисника - Деанонімізація - Підготовка доказів - Передача в слідчі органи |

1. **SLA - часові рамки**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Рівень | Виявлення | Реагування | Усунення | Відновлення |
| Критичний | <=15 хв | <=1 год | <=4 год | <=8 год |
| Середній | <=1 год | <=4 год | <=12 год | <=24 год |
| Низький | <=4 год | <=24 год | <=48 год | <=72 год |
| **Скрите реагування** | **Моніторинг** | | **Деанонімізація** | |
| Критичний | <=15 хв | | <=3 год | |
| Середній | <=1 год | | <=5 год | |
| Низький | <=4 год | | <=8 год | |

\*часові рамки можуть коригуватися в залежності від ситуації чи критичності підприємства

1. **Виявлення інцидентів**

*Інструменти*

|  |  |
| --- | --- |
| **Інструмент** | **Призначення** |
| SIEM (Splunk, QRadar) | Централізований збір, кореляція та аналіз логів для виявлення інцидентів, аномалій та порушень політик. |
| IDS/IPS (Snort, Suricata) | Виявлення (IDS) та блокування (IPS) несанкціонованої або шкідливої мережевої активності в реальному часі. |
| EDR (CrowdStrike) | Моніторинг кінцевих точок, виявлення загроз, ізоляція заражених пристроїв та форензичний аналіз. |
| Honeypot | Імітація вразливих систем для виявлення атак, збору інформації про методи зловмисників та їх деанонімізації. |
| Threat Intelligence | Збір, аналіз та застосування даних про актуальні загрози для проактивного захисту та адаптації політик. |
| Red Team (симуляції) | Проведення контрольованих атак для тестування стійкості систем, виявлення слабких місць та навчання персоналу. |

*Класифікація інцидентів*

|  |  |
| --- | --- |
| **Рівень** | **Критерії** |
| Високий | Витік даних , штрафи, загублена репутація, недовіра партнерів |
| Середній | Частковий вплив |
| Низький | Технічні помилки |

1. **Комунікаційний план**

Типи повідомлення:

*Тривожне повідомлення*

* Оперативне інформування ключових осіб (менеджер, SOC, юридичний відділ, окремі випадки фізична охорона) про виявлений інцидент.

*Регулярне оновлення*

* Статус реагування, прогрес усунення, ризики. Внутрішні канали: email, Slack, внутрішній портал.

*Фінальні звіти*

* Після завершення реагування - технічний, юридичний та комунікаційний звіт.

*\*\*\* Скрите реагування*

* *Внутрішнє використання:* повідомлення лише вузькому колу (SOC, Red Team, юридичний представник, окремі випадки фізична охорона ). Без зовнішнього розголосу до завершення деанонімізації.

Визначення ключових повідомлень

|  |  |
| --- | --- |
| **Аудиторія** | **Повідомлення** |
| **Співробітники** | Інструкції щодо безпеки, зміни в політиках, уникнення паніки. |
| **Клієнти** | Пояснення ситуації, заходи захисту, компенсації (якщо потрібно). |
| **Медіа** | Контрольований прес-реліз, уникнення спекуляцій. |
| **Регулятори** | Повідомлення згідно з вимогами GDPR, ЗУ «Про захист персональних даних». |
| **Скрите реагування** | Немає зовнішніх повідомлень до завершення внутрішнього розслідування. |

1. **План відновлення**

*Загальні принципи:*

* Відновлення починається лише після повної ізоляції та завершення аналізу.
* Пріоритет - цілісність даних, безпечне середовище, контроль доступу.
* Документування всіх дій
* Відновлення включає тестування, перевірку, моніторинг
* Після відновлення - оновлення політик та навчання персоналу

*Процедури:*

Резервні копії:

* *Оцінка*: визначення обсягу втрат, перевірка цілісності резервних копій
* *Відновлення*: відновлення даних на нових або очищених системах.
* *Перевірка*: тестування працездатності, перевірка відповідності.
* *Тестування*: навантажувальне тестування, перевірка інтеграцій.
* *Документування*: запис усіх дій, оновлення журналів та звітів.

Заміна обладнання/ПЗ:

* *Оцінка:* визначення пошкоджених компонентів, аналіз вартості заміни
* *Заміна*: закупівля, встановлення нового обладнання або ПЗ
* *Перевірка*: тестування сумісності, безпеки, продуктивності.
* *Документація*: оновлення інвентаризації, технічної документації.

Перевірка систем після відновлення:

* *Перевірки*: сканування на вразливості, перевірка конфігурацій.
* *Моніторинг*: активне спостереження за поведінкою системи.
* *Аналіз*: виявлення залишкових ризиків, корекція налаштувань
* *Документування*: фіксація результатів, оновлення політик.

Великі інциденти:

* *Аналіз впливу*: оцінка фінансових, репутаційних, юридичних наслідків.
* *Комунікація*: повідомлення клієнтів, партнерів, регуляторів.
* *Оцінка вдосконалення*: визначення слабких місць, оновлення політик, навчання персоналу.

1. **Оцінка, стримування та розслідування**

Попереднє стримування:

* Виявлення інциденту - негайна ізоляція.
* У випадку скритого реагування - ***моніторинг без втручання***, логування дій зловмисника.
* Деанонімізація
* У випадку фізичного проникнення - ***спостереження, документування***, передача охороні.

Розслідування:

* *Форензичний аналіз*: логів, пам’яті, мережевої активності.
* *Виявлення* джерела атаки методів проникнення
* *Деанонімізація* через поведінковий аналіз.
* *Підготовка* доказової бази для юридичних дій.

*\*\*\*Внутрішнє використання:*

*У випадках шпигунства, фізичного проникнення, виявлення додаткового обладнання - реагування здійснюється* ***непомітно****, з метою* ***виявлення та фіксації дій зловмисника****, перш ніж передати справу охороні або слідчим органам.*

1. **Реагування на фізичні загрози та внутрішнє шпигунство**

*8.1. Потрапляння невідомих осіб до серверних приміщень (внутрішнє використання)*

* Не вступати у відкриту конфронтацію
* Активувати приховане відеоспостереження
* Задокументувати дії особи (переміщення, доступ до обладнання)
* Повідомити фізичну охорону та SOC
* Після фіксації - ізоляція доступу, допит(звучить грубо, але…), юридична оцінка.

*8.2. Підпал або фізичне знищення серверної*

Пожежа/знищення обладнання

* Активація пожежної сигналізації
* Евакуація персоналу
* Повідомлення аварійних служб
* Ізоляція електроживлення
* Перевірка резервних копій
* Перехід на резервні вузли/хмарні сервіси
* Документування втрат та юридичне реагування

*8.3. Виявлення додаткового обладнання (шпигунство)*

Виявлення невідомого пристрою (внутрішнє користування)

* **Не демонтувати одразу**
* Активувати приховане логування трафіку
* Встановити моніторинг активності пристрою
* Виявити джерело передачі даних
* Деанонімізувати зловмисника
* Після фіксації - вилучення, юридичне реагування

*8.4.* *Роль фізичної охорони*

|  |  |
| --- | --- |
| **Обов’язки** | **Опис** |
| **Відеоспостереження** | Постійний моніторинг критичних зон |
| **Контроль доступу** | Перевірка посвідчень, обмеження доступу |
| **Реагування** | Негайне втручання у разі фізичної загрози |
| **Підтримка розслідування** | Надання записів, свідчень, участь у внутрішньому розслідуванні |
| **Збереження доказів** | Фіксація дій сторонніх осіб, збереження обладнання до передачі слідчим |

**Висновок**

Ми охопили не всі варіанти інцидентів. Також можна зазначити певні категорії інцидентів, які можуть статися на підприємстві. Ось декілька з них.

*Кіберінциденти:*

* **DDoS / DoS атаки**
* **Витік персональних даних**
* **Шкідливе програмне забезпечення (віруси, трояни, бекдори)**
* **Фішинг / соціальна інженерія**
* **Компрометація облікових записів (включно з привілейованими)**
* **Несанкціонований доступ до систем/мережі**
* **Використання вразливостей у ПЗ/ОС**
* **Зміна конфігурацій без дозволу**
* **Використання незахищених протоколів (FTP, Telnet)**
* **Встановлення сторонніх додатків або скриптів**
* **Використання корпоративної інфраструктури для атак на інші ресурси (outbound attack)**
* **Викрадення або підробка цифрових сертифікатів/ключів**
* **Зміна логів або спроба приховати сліди атаки (log tampering)**

Інциденти *пов’язані* з людським фактором

* **Помилкове видалення або зміна критичних даних**
* **Ненавмисне розголошення конфіденційної інформації**
* **Порушення політик доступу або безпеки**
* **Використання слабких паролів/спільних облікових записів**
* **Ігнорування оновлень/патчів**
* **Неправильне налаштування безпеки (misconfiguration)**

*Фізичні і технічні інциденти*

* **Потрапляння сторонніх осіб до серверних приміщень**
* **Підпал/знищення обладнання**
* **Виявлення шпигунського обладнання**
* **Відмова обладнання (сервери, маршрутизатори, комутатори)**
* **Відмова електроживлення/UPS/охолодження**
* **Пошкодження кабельної інфраструктури/оптоволокна**
* **Крадіжка пристроїв (ноутбуки, телефони, флешки)**
* **Втручання в систему відеоспостереження або контролю доступу**

*Юридичні та репутаційні інциденти*

* **Порушення вимог GDPR або ЗУ «Про захист персональних даних»**
* **Несвоєчасне повідомлення регуляторів про інцидент**
* **Інцидент, що спричинив медійний резонанс або втрату довіри клієнтів**
* **Витік контрактної або фінансової інформації**
* **Інцидент, що спричинив штраф або судовий позов**