План реагування на інциденти кібербезпеки для телекомунікаційної компанії "УкрТелеком"

1 Вступ

1.1 Мета документу

Цей план реагування на інциденти кібербезпеки розроблено для телекомунікаційної компанії "УкрТелеком" з метою запобігання, виявлення, реагування та відновлення після інцидентів інформаційної безпеки. Документ встановлює чіткі процедури та розподіл обов'язків для забезпечення швидкого та ефективного реагування на загрози безпеки, мінімізації їх впливу на бізнес-операції та захисту даних клієнтів.

1.2 Обсяг застосування

Цей план застосовується до всіх підрозділів ТОВ "УкрТелеком", включаючи технологічні системи, мережі передачі даних, системи зберігання та обробки даних клієнтів, а також будь-які інші інформаційні активи, що належать компанії або знаходяться під її управлінням.

1.3 Життєвий цикл плану

Цей план є живим документом, який підлягає регулярному оновленню. Перегляд та тестування будуть проводитися щонайменше раз на півроку, а також після кожного серйозного інциденту, зміни інфраструктури або нормативних вимог.

2 Команда реагування на інциденти: ролі та обов'язки

Команда реагування на інциденти (КРІ) "УкрТелеком" формується з фахівців різних підрозділів для забезпечення комплексного підходу до управління інцидентами безпеки. До складу команди входять: (https://www.vpnunlimited.com/ua/help/cybersecurity/incident-response-plan?srsltid=AfmBOoprjuxd1u5hnIaq7k1ir9fe7g4lY_4buIarGzTq2aeI3Kj_O8o5)

Таблиця 1: Ролі та обов'язки команди реагування на інциденти

Роль	Обов'язки	Відповідальність
Менеджер інцидентів	Загальна координація роботи КРІ, прийняття стратегічних рішень, зв'язок з вищим керівництвом	Координація всіх етапів реагування, затвердження ресурсів, звітування перед керівництвом
Аналітики безпеки (рівні 1-2)	Первинний аналіз сповіщень, розслідування інцидентів, виконання процедур стримування	Моніторинг загроз, аналіз вразливостей, класифікація інцидентів, технічне розслідування
Аналітики безпеки (рівень 3)	Глибинний аналіз складних інцидентів, полювання на загрози, розробка контрзаходів	Розслідування складних інцидентів, проактивний пошук загроз, аналіз вразливостей
IT-персонал	Відновлення систем, виправлення конфігурацій, резервне копіювання та відновлення даних	Технічна реалізація заходів стримування та відновлення, підтримка роботи систем
Представник юридичного відділу	Оцінка юридичних ризиків, дотримання нормативних вимог, взаємодія з правоохоронними органами	Дотримання законодавства про захист даних, підготовка юридичних документів, консультації
PR-фахівець	Комунікації з зацікавленими сторонами, управління репутацією, робота з ЗМІ	Розробка комунікаційних повідомлень, взаємодія з клієнтами та громадськістю

3. Процедури реагування на інциденти

3.1 Загальна структура реагування

Процес реагування на інциденти в "УкрТелеком" будується на стандартному життєвому циклі, що включає підготовку, виявлення та аналіз, стримування, усунення, відновлення та пост-інцидентний аналіз. Для кожного типу інциденту розроблені детальні процедури, що забезпечують послідовність та ефективність дій.

3.2 Витік персональних даних

•**Виявлення та аналіз**: Негайно ізолювати уражені системи від мережі для запобігання подальшого витоку. Зберегти всі журнали та артефакти для подальшого аналізу. Визначити обсяг та характер витоку (які саме дані, хто зачіплений).
•**Стримування та усунення**: Блокувати скомпрометовані облікові записи. Оновити паролі доступу. Встановити та усунути вразливість, що призвела до витоку. Провести аналіз на наявність інших систем, які мають аналогічні вразливості.
•**Відновлення**: Відновити системи з чистих резервних копій, якщо це необхідно. Впровадити додаткові заходи безпеки для запобігання майбутнім інцидентам. Перевірити цілісність та безпеку систем перед повним відновленням роботи.

3.3 DDoS-атака

•**Виявлення та аналіз**: Ідентифікувати характер атаки (об'ємна атака, атака на рівні додатків). Визначити уражені сервіси та рівень деградації послуг.
•**Стримування та усунення**: Активувати послуги DDoS-мітігації від постачальника послуг. Переконфігурувати мережеве обладнання для блокування шкідливого трафіку. Перенаправити трафік через систему очищення.
•**Відновлення**: Поступово відновити нормальний трафік після завершення атаки. Продовжувати моніторинг для виявлення залишкових ефектів або повторних атак. Оновити правила фаєрволу та системи виявлення вторгнень на основі отриманих даних.

3.4 Виявлення шкідливого ПЗ

•**Виявлення та аналіз**: Від'єднати уражені системи від мережі. Визначити тип шкідливого ПЗ (ransomware, троян, бекдор тощо) та ступінь поширення.
•**Стримування та усунення**: Видалити шкідливе програмне забезпечення з усіх інфікованих систем. Сканування всієї мережі на наявність аналогічних інфекцій. Оновити антивірусні сигнатури.
•**Відновлення**: Відновити дані з резервних копій, якщо це необхідно. Перевстановити операційні системи на повністю уражених машинах. Провести перевірку всіх систем на наявність залишкових компонентів шкідливого ПЗ.

4. Класифікація інцидентів та часові рамки реагування

4.1 Критерії класифікації

Інциденти класифікуються за рівнем серйозності на основі кількох ключових факторів:

•**Критичний (Рівень 3)**: Значні фінансові втрати (понад 500 тис. грн), порушення роботи критичних послуг, масштабний витік даних клієнтів, серйозні репутаційні збитки, порушення законодавства з ризиком великих штрафів.
•**Високий (Рівень 2)**: Помірні фінансові втрати (100-500 тис. грн), порушення роботи некритичних послуг, обмежений витік даних, помірний репутаційний ризик.
•**Середній (Рівень 1)**: Незначні фінансові втрати (до 100 тис. грн), локальне порушення роботи систем, мінімальний репутаційний ризик, відсутність порушень законодавства.

4.2 Цільові показники відновлення (RTO та RPO)

Для кожного класу інцидентів встановлені цільові показники відновлення, що базуються на концепції RTO (Recovery Time Objective) та RPO (Recovery Point Objective):

•**RTO (Цільовий час відновлення)**: Максимально допустимий час, протягом якого система може бути недоступною.
•**RPO (Цільова точка відновлення)**: Максимальний період часу, протягом якого можливі втрати даних у разі інциденту.

Таблиця 2: Часові рамки реагування на інциденти

Рівень інциденту	Час реагування	Цільовий час відновлення (RTO)	Цільова точка відновлення (RPO)	Необхідні дії
Критичний (3)	≤ 15 хвилин	≤ 4 години	≤ 15 хвилин	Негайне стримування, залучення всієї команди, сповіщення керівництва
Високий (2)	≤ 1 години	≤ 24 години	≤ 4 години	Швидке стримування, залучення необхідних фахівців, обмежене сповіщення
Середній (1)	≤ 4 години	≤ 3 діб	≤ 24 години	Планове усунення, обмежене залучення фахівців, внутрішня документація

5. Процедури виявлення інцидентів

5.1 Інструменти моніторингу та виявлення

Для виявлення аномалій та потенційних інцидентів безпеки в "УкрТелеком" використовується комплекс інструментів та технологій:

•**SIEM (Security Information and Event Management)**: Система керування інформацією та подіями безпеки, яка агрегує та аналізує журнали з різних джерел (мережевих пристроїв, серверів, застосунків) для виявлення підозрілих активностей .
•**IDS/IPS (Системи виявлення/запобігання вторгненням)**: Мережеві та хост-системи для ідентифікації відомих векторів атак та блокування підозрільної мережевої активності.
•**Антивірусне програмне забезпечення**: Системи для виявлення та блокування шкідливого програмного забезпечення на кінцевих пристроях та серверах.
•**Системи моніторингу мережевого трафіку**: Інструменти для аналізу аномалій у мережевому трафіку, що можуть вказувати на DDoS-атаки або несанкціоновану передачу даних.

5.2 Процес виявлення та ескалації

Процес виявлення та ескалації інцидентів будується на багаторівневій моделі SOC (Security Operations Center):

•**Аналітик 1-го рівня**: Проводить первинну оцінку сповіщень від систем моніторингу, фільтрує хибно-позитивні спрацьовування та ініціює інциденти для більш глибокого аналізу.
•**Аналітик 2-го рівня**: Займається глибшим розслідуванням інцидентів, визначає масштаби компрометації, проводить початкове стримування загроз.
•**Аналітик 3-го рівня**: Займається полюванням на загрози, розслідуванням складних та цілеспрямованих атак, розробкою контрзаходів для запобігання майбутнім інцидентам.

6. Комунікаційний план

6.1 Загальні принципи комунікації

Ефективна комунікація є критично важливою складовою успішного управління інцидентами. В "УкрТелеком" діють наступні принципи комунікації під час інцидентів :

•**Чіткість та прозорість**: Всі повідомлення мають бути зрозумілими, точними та відповідати фактичному стану речей.
•**Своєчасність**: Інформація має надходити до зацікавлених сторін у визначені часові рамки.
•**Відповідність аудиторії**: Зміст та форма повідомлення мають адаптуватися до конкретної аудиторії (регулятори, клієнти, ЗМІ тощо).
•**Безпека каналів зв'язку**: Використання лише безпечних каналів зв'язку для передачі конфіденційної інформації.

6.2 Матриця комунікації

Таблиця 3: Матриця комунікації під час інцидентів

Зацікавлена сторона	Метод комунікації	Частота оновлення	Відповідальність
Внутрішні стейкхолдери	Електронна пошта, система екстреного сповіщення, месенджери	При отриманні нової важливої інформації	Менеджер з інцидентів
Клієнти	Офіційний веб-сайт, електронна пошта, SMS-сповіщення	При значних змінах статусу, але не рідше ніж кожні 4 години для критичних інцидентів	PR-фахівець
Державні органи	Офіційні листи, телефонні дзвінки	Відповідно до вимог законодавства	Юридичний відділ
ЗМІ	Пресс-релізи, офіційні заяви через веб-сайт	При істотних змінах ситуації, що потребують публічного розголошення	PR-фахівець
Партнери	Електронна пошта, телефонні дзвінки	За потреби з метою координації	Менеджер з інцидентів

6.3 Шаблони повідомлень

6.3.1 Шаблон повідомлення для клієнтів (витік даних)

***Тема**: Важлива інформація щодо захисту ваших даних у "УкрТелеком"*

"Шановний(а) клієнте!

Із найвищим пріоритетом повідомляємо, що [дата] нами було виявлено технічну аномалію, яка могла призвести до несанкціонованого доступу до окремих категорій ваших даних. Ми вжили негайних заходів для усунення цієї аномалії та залучили спеціалістів з кібербезпеки для проведення повного розслідування.

Рекомендуємо вам: [конкретні рекомендації].

Додаткову інформацію та оновлення ви можете значати на нашому офіційному сайті [посилання]. Гаряча лінія з питань інциденту: [номер телефону].

Приносимо вибачення за незручності та дякуємо за розуміння.

З повагою,
Команда безпеки "УкрТелеком""

7 План відновлення

7.1 Загальні принципи відновлення

Процедури відновлення в "УкрТелеком" базуються на концепції DRP (Disaster Recovery Plan) та є частиною загальної стратегії безперервності бізнесу (Business Continuity Plan). Відновлення проводиться після повного усунення загрози та включає наступні етапи:

- **Оцінка збитків**: Визначення повного обсягу ушкоджень, заподіяних інцидентом.
- **Пріоритизація**: Відновлення систем відповідно до їх критичності для бізнес-операцій.
- **Відновлення даних**: Використання резервних копій для відновлення втрачених або пошкоджених даних.
- **Тестування**: Перевірка коректності роботи відновлених систем перед повним введенням в експлуатацію.
- **Моніторинг**: Підвищена увага до відновлених систем для виявлення можливих аномалій.

7.2 Процедури відновлення для різних типів інцидентів

7.2.1 Відновлення після витоку даних

- Перевірка цілісності систем зберігання даних.
- Оновлення механізмів контролю доступу та шифрування даних.
- Впровадження додаткових заходів моніторингу доступу до конфіденційних даних.
- Проведення аудиту безпеки для виявлення потенційних вразливостей.

7.2.2 Відновлення після DDoS-атаки

- Поступове зняття заходів мітігації після завершення атаки.
- Аналіз ефективності заходів захисту та внесення коректив в конфігурації.
- Оновлення правил мережевих екранів та систем виявлення вторгнень.
- Координація з интернет-провайдерами для впровадження додаткових заходів захисту.

7.2.3 Відновлення після інфекції шкідливим ПЗ

- Відновлення систем з чистих резервних копій, якщо це необхідно.
- Повне сканування всієї мережі на наявність залишкових компонентів шкідливого ПЗ.
- Оновлення антивірусних баз та сигнатур.
- Переконфігурація систем для усунення вразливостей, що були використані для проникнення.

7.3 Контроль якості відновлення

Після завершення процесу відновлення проводиться контроль якості, який включає:

- Перевірку цілісності та доступності даних.
- Тестування функціональності всіх критичних бізнес-процесів.
- Перевірку роботи механізмів безпеки та моніторингу.
- Підтвердження відповідності нормативним вимогам.

8 Рекомендації щодо вдосконалення плану

Для поглиблення розуміння практичного застосування теоретичних знань у сфері кібербезпеки рекомендовано:

- **Аналіз реальних інцидентів**: Досліджувати реальні інциденти кібербезпеки в телекомунікаційному секторі України та світу, використовуючи відкриті джерела. Аналізувати ефективність застосованих заходів реагування та адаптувати найкращі практики для вдосконалення цього плану.
- **Регулярне тестування**: Проводити навчальні симуляції інцидентів для перевірки ефективності плану та підготовки команди. Тестування має включати різні сценарії та проводитися не рідше ніж раз на квартал.
- **Безперервне оновлення**: План має переглядатися та оновлюватися відповідно до змін в інфраструктурі, з'явлення нових загроз та змін в законодавстві.
- **Проактивний підхід**: Перехід від реактивного до проактивного реагування шляхом використання розвідки загроз, автоматизації та аналітики на основі штучного інтелекту для виявлення та пом'якшення загроз до того, як вони можуть завдати шкоди.
- Розвиток культури безпеки: Заохочення співробітників до негайного повідомлення про підозрілі події без страху покарання, що є критично важливим для своєчасного виявлення інцидентів.