**СЦЕНАРІЙ СИТУАЦІЙНОЇ ВПРАВИ [Назва вправи]**

# Модуль 1: Обмін інформацією в рамках попередньої підготовки

## Сценарій

## [Країна, місто]

### [Дата], [час]

Минув рік відтоді, як розробник вашої поточної операційної системи оголосив, що більше не розроблятиме патчі безпеки для вашої операційної системи. Останній патч безпеки було встановлено минулого тижня. Цю вразливість було виявлено під час щорічного оцінювання ризиків, котре ви нещодавно завершили.

Працівник організації повідомляє своєму безпосередньому керівнику, що вночі з його автомобіля викрали робочий ноутбук. Цей комп’ютер містив конфіденційну інформацію.

На сайтах CERT-UA та Держспецзв’язку опубліковано сповіщення щодо появи нового варіанту програми-вимагача. Ця програма-вимагач використовується в атаці, спрямованій на органи влади, а також підприємства приватного сектору.

Один з керівників компанії отримує листа від співробітника управління захисту інформації одного з підрозділів компанії (в листі вказана корпоративна пошта) щодо ситуації з обладнанням, отриманим в рамках матеріально-технічної допомоги.

Керівник доручає відповідальному за матеріально-технічне забезпечення розібратися в ситуації.

## Керівник та відповідальний підлеглий за матеріально-технічне забезпечення додані до мереж одне одного на вебсайтах домену Організації. В електронному листі зазначається, що співробітник управління захисту інформації нещодавно помітив спроби неправомірного використання обладнання, і рекомендує переглянути матеріали, що підтверджують дану інформацію. Відповідальний за матеріально-технічне забезпечення натискає на посилання, наведене в електронному листі та його перенаправляє на особисте хмарне середовище, посилання на яке та файли виглядають як справжні. Відповідальний за матеріально-технічне забезпечення не вважає електронний лист підозрілим.

## Запитання для обговорення

1. Чи буде ідентифіковано як кіберінцидент або кіберподію будь-яку із подій, описаних у цьому модулі? Якщо так, то як саме буде здійснюватися реагування?
2. Про яку з вишченаведених подій Ваша організація повідомить CERT-UA (А Міненерго?)? В яких часових рамках? Чи існує в вашій організації документ, який регламентує (визначає порядок) інформування уповноважених та правоохоронних органів? Яким коліром буде марковано таке/такі повідомлення у відповідності до наведених вишче подій (згідно TLP протоколу)?
3. Які заходи із блокування можливих наслідків у випадку кражі робочого ноутбуку будуть проведені?
4. З яких ще джерел ваша організація отримує інформацію про загрози кібербезпеці? Наприклад ви отримуєте інформацію від НКЦК, CERT-UA, Служби безпеки України (СБУ), Департамент кіберполіції Національної поліції України, громадських організацій, звіти з відкритих джерел, від постачальників послуг з управління безпекою, постачальників або розробників обладнання, ПЗ від інших установ чи організацій?
	1. Яка інформація щодо кіберзагроз є найкориснішою?
	2. Інформація, яку ви отримуєте, надходить своєчасно та є дієвою?
	3. Хто відповідає у вашій організації за збір та співставлення інформації?
5. Чи проводить ваша організація базове навчання з кібербезпеки та/або підвищення рівня обізнаності щодо безпеки у сфері ІТ для всіх користувачів (включаючи менеджерів та керівників вищої ланки)?
	1. Наскільки часто проводиться навчання?
	2. Чи охоплює навчання наступні питання:
		1. Огляд політик прийнятного використання та політик у сфері ІТ/ІБ організації,
		2. Рівень обізнаності щодо відомих кіберзагроз,
		3. Порядок та процедури встановлення пароля, а також
		4. До кого звертатися та як повідомляти про підозрілу діяльність?
	3. Чи необхідно проходити певне навчання для отримання доступу до мережі?
	4. Яке навчання з питань безпеки проводить ваша організація або вимагає від ІТ-персоналу і служб/підрядників/постачальників, які мають доступ до інформаційних систем вашої організації, згідно з договором/контрактом?
	5. Як часто вони проходять навчання?
6. Як працівники повідомляють про підозри щодо спроб фішинг-атаки?
	1. Яких заходів вживає ваш підрозділ ІБ, коли повідомляють про підозрілі електронні листи?
	2. Чи існують офіційні політики чи плани, яких слід дотримуватися?
	3. Чи проводить ваша організація самооцінку щодо фішингу?
	4. Чи використовується навчальна платформа з створення та розсилки фішингових повідомлень в Вашій організації?
7. Чи проводила ваша організація оцінювання кіберризиків, щоб визначити загрози та вразливості, характерні для організації?
	1. Які ваші найвагоміші загрози та вразливості?
	2. Які ризики кібербезпеки є найвищими для вашої організації?
8. Чи є у вашому ІТ-відділі план управління оновленнями / внесенням виправлень (патч-менеджменту)? Якщо так, то:
	1. Чи проводиться оцінювання ризиків на всіх серверах у мережі?
	2. Чи існують процеси для проактивного оцінювання критичності кожного сервера та можливості застосування оновлень/виправлень (патчів) для застосунків?
	3. Чи містить цей план стратегію управління ризиками, яка враховує нижченаведені міркування?
		1. Ризики невнесення виправлень щодо повідомлених вразливостей,
		2. Тривалий час простою,
		3. Погіршення функціональності, і
		4. Втрата даних?

# Модуль 2: Реагування на інцидент

## Сценарій

### [Дата], [час]

### Ваш ІТ-персонал регулярно переглядає журнали (лог-файли) системи виявлення атак/вторгнень і виявляє незвичний трафік на портах принтера вашої організації. Через порти принтера значна кількість даних передається на зовнішні IP-адреси.

### Ваші працівники помічають кілька незначних змін на вебсайті організації. Вони також відзначають, що посилання, котре часто використовувалося, відтепер спрямовує користувачів на вебсайт, не пов’язаний із вашою організацією.

### По всій вашій організації на комп’ютерах з’являються червоні екрани. Здається, що всі вони були заражені однією і тією самою програмою-вимагачем. На екранах відображається повідомлення з вимогою сплатити викуп у біткоїнах на суму приблизно 100 000 доларів США за отримання ключа дешифрування із попередженням, що термін дії ключа закінчиться, якщо відповідний платіж не надійде протягом 48 годин.

### Дослідник у галузі безпеки знаходить у даркнеті серію публікацій та зв’язується з вашою організацією. Дослідник вважає, що ці дописи, котрі нібито опубліковані відомою хакерською групою, є справжніми і що зловмисники отримали доступ до інформації, яка дає змогу ідентифікувати особу (персональні данні), зокрема <ідентифікаційні коди, дані щодо банківських рахунків і транзитні маршрутні номери (коди банку, МФО) тощо>. Група хакерів надала незначну кількість записів даних на підтвердження своїх заяв, і готова продати інформацію за «відповідну ціну».

### Запитання для обговорення

1. В який спосіб у вашій організації проводитимуть оцінювання кіберінцидентів? У вашій організації визначені рівні критичності кіберінциденту та/або критерії для підвищення його рівня критичності?
2. Яких заходів вживатимуть на цьому етапі? Хто їх вживатиме?
3. Які сповіщення буде зроблено? Розгляньте внутрішні сповіщення (наприклад, інформування керівництва) і зовнішні сповіщення (наприклад, до органів правопорядку, урядових партнерів, уповноважених органів, тощо).
4. Як виглядає базова активність мережі у вашій організації? Як ви могли б відрізнити нормальний трафік від ненормального?
5. Ви сплатите викуп?
	1. Хто приймає рішення?
	2. Як виглядатиме процес?
	3. Які переваги/недоліки рішення сплатити викуп?
	4. Якими будуть потенційні політичні наслідки?
	5. З якими зовнішніми партнерами/ організаціями вам необхідно зв’язатися?
6. Які можливості та ресурси вам потрібні для реагування на цю низку інцидентів?
	1. Від яких внутрішніх ресурсів ви залежите?
	2. Чи достатньо вам ресурсів, які у вас є на поточний момент?
	3. Чи є у вашій організації працівники, відповідальні за реагування на інциденти, або призначена команда (група) реагування на кіберінциденти?
		1. Якщо так, яких показників чи етапу має бути досягнуто (рівня ескалації), щоб було приведено у стан готовності та залучено особовий склад, який бере участь у реагуванні на інциденти? Цей сценарій досягає цих показників чи етапу (рівня ескалації)?
		2. Хто відповідає за приведення у стан готовності та залучення особового складу, котрий бере участь у реагуванні на інциденти, та за яких обставин це відбувається?
		3. Як на це впливає час доби? Комендантська година? Необхідність застосувати транспорт вночі?
		4. Якими є функції та обов’язки команди (групи) реагування на кіберінциденти/відповідного особового складу?
	4. До кого ви звертаєтеся, якщо вам потрібна додаткова допомога з боку третіх сторін (сторонніх організацій)? Чи є попередні договори про співробітництво/надання послуг, підписані договори про конфіденційність, нерозголошення (NDA) з такими організаціями?
7. Що вас непокоїть в аспекті зв’язків із громадськістю?
	1. Хто відповідає за координацію інформаційного повідомлення для громадськості? Чи є цей процес частиною будь-якого сформованого плану?
	2. Як саме ваш структурний підрозділ відреагує на повідомлення у ЗМІ?
	3. Якою інформацією ви ділитеся з громадськістю? Чи існує заборона для працівників коментувати такі події, правила, або політика опублікування інформації?
	4. Персонал служби зв’язків із громадськістю (відділу забезпечення доступу до публічної інформації) пройшов навчання з питань управління повідомленнями, пов’язаними з кіберінцидентами/кібератаками?
	5. Чи є у вашому структурному підрозділі підготовлені проєкти заяв для представників ЗМІ?
	6. Чи є у вашому структурному підрозділі персонал, навчений управляти вашою «присутністю» в соціальних мережах?
8. Який вплив матиме продаж конфіденційної інформації чи інформації, що дає змогу ідентифікувати особу (персональні дані), на вашу діяльність із реагування та відновлення?
	1. Відділ ІТ/ІБ попередить органи влади (хто з них)? Чи змінилися ваші пріоритети у сфері зв’язків із громадськістю?
	2. Чи це призведе до додаткових юридичних або нормативних сповіщень.