USAID
FROM THE AMERICAN PEOPLE

РОЗРОБКА ОРГАНІЗАЦІЙНОГО ПЛАНУ РЕАГУВАННЯ НА ІНЦИДЕНТ

Як організаціям правильно реагувати на загрози

Цей документ підготовлений на замовлення USAID. Його самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цьому документі, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

МОДУЛЬ І - ВСТУП

В сучасному світі є очевидним той факт, що все більше компаній, включно із малими та середнього розміру організаціями, потребують плану реагування на загрози у сфері кібербезпеки. Жодна організація, незалежно від її розміру, не є захищеною від загроз у кібер просторі, і тому потребує встановленого плану дій, який негайно виконується після порушення цілісності системи безпеки, та є критичним для зменшення витрат від інциденту та збитків для репутації компанії.

Звісно, існують сотні можливих випадків – не кажучи вже про різні варіанти розвитку подій – коли все має скластися ідеально і спрацювати бездоганно, щоб реагування на інцидент було успішним. Деякі компанії, особливо ті, котрі ще не мають досвіду боротьби з серйозними інцидентами у галузі безпеки, не знають, з чого починати, а тим більше – як розставити пріоритети.

Інцидент – це коли, а не «якщо», стається компрометація або порушення системи безпеки організації. Підготовка Команди реагування на комп'ютерні інциденти (англ. Computer Incident Response Team (CIRT)) шляхом планування, комунікації та відпрацювання процесів реагування на інцидент, дасть можливість отримати досвід, необхідний у ситуації, коли у вашій організації такий інцидент станеться.

Кожен етап від підготовки до отриманих уроків потрібно виконувати послідовно, оскільки кожен з них спирається на інший. Наступні етапи стануть базовою основою для виконання заходів для реагування на інциденти та дозволять створити власний план реагування на інциденти.

ЗАГАЛЬНІ ПОНЯТТЯ

Реагування на інциденти порушення комп‘ютерної безпеки стали важливим компонентом IT програм. Оскільки ефективне реагування на інциденти є складним, воно вимагає значного планування та ресурсів.

Цей модуль допомагає особам, що навчаються, отримати вміння у сфері реагування на порушення комп‘ютерної безпеки та вчить раціонального та ефективного поводження під час таких інцидентів. Модуль надає інструкції для правильного поводження під час інцидентів, а саме аналізу даних, що мають відношення до інцидентів, та визначення належного реагування на кожен інцидент. Цим інструкціям можна слідувати, незалежно від виду використовуваних програмних платформ, операційних систем, протоколів або додатків.

ПІДГОТОВКА

Ця фаза, як зазначено у самій назві, стосується підготовки команди до того, щоб вона могла впоратися із інцидентом у найкоротші терміни. Складність інциденту може варіюватися від будь-чого, наприклад, від відключення електроенергії або відмови обладнання, до екстремальних випадків, таких як порушення організаційної політики незадоволеними працівниками або проплачені хакерські атаки (Бейтліх, 2005).

Незалежно від причини інциденту, фаза підготовки є вирішальною порівняно зі всіма іншими, оскільки саме вона визначає, наскільки швидко ваша команда буде здатна реагувати у випадку критичної ситуації. На цьому етапі необхідно впровадити кілька ключових елементів, з метою пом'якшення будь-яких потенційних проблем, які можуть перешкодити спеціалісту впоратися з інцидентом. Якщо коротко, слід здійснити наступне:

1. Політика – являє собою записаний набір принципів, правил та практик в межах організації. Це один з базових елементів, на який спираються усі інструкції щодо дій на випадок виникнення інциденту в організації. Банер, що з'являється під час входу, це спосіб гарантувати, що особи, які намагаються увійти в мережу організації, будуть знати, що очікується при використанні інформаційних ресурсів організації; наприклад, у банері для входу (залежно від місцевої юрисдикції щодо конфіденційності) може бути зазначено, що всі дії будуть відстежуватися, а до будь-яких неавторизованих користувачів можуть застосовуватись цивільні або кримінальні санкції тощо. Без чіткої політики організація може залишитись юридично вразливою для судових позовів, наприклад, звільнення працівника за перегляд незаконного матеріалу на роботі, коли в організації не було політики проти такої поведінки, це дало можливість зазначеній особі подати позов про неналежний судовий позов (Ньюмен, 2007).

2. План реагування/Стратегія. Після встановлення політики організації слід розробити план/стратегію на випадок інцидентів. Визначення пріоритетів щодо інцидентів повинно базуватися на сфері їх впливу на організацію (Методи реагування на інцидент, 2008), наприклад, одне автоматизоване робоче місце, що вийшло з ладу, може бути визнано неважливим інцидентом, у той час як сервер, що не працює, може вважатися інцидентом помірного рівня важливості (за умови, що існують резервні сервери на випадок відмови основного), а викрадення даних безпосередньо з відділу кадрів організації, що мають привілейований доступ до інформації, вважатиметься інцидентом високого рівня важливості. Встановлення пріоритетів щодо типів інцидентів на основі сфер їх впливу на організацію може допомогти створити умови для усвідомленої підтримки з боку менеджменту, оскільки без підтримки менеджменту CIRT не отримає необхідних ресурсів для того, щоб належним чином впоратися із кризою.

3. Комунікація. Наявність плану комунікації є необхідною, оскільки може виникнути потреба контактувати із специфічними особами під час інциденту. Уся CIRT повинна знати, з ким контактувати, коли належить контактувати і чому. Наприклад, о 12:31 відмовляє система онлайн замовлень популярного сайту у вихідний під час сезону покупок, і ніхто не може отримати доступ до сайту. Є сенс зв'язатися з технічними експертами у даній галузі, щоб відновити систему і налагодити її роботу, а також з менеджментом, щоб керівництво володіло актуальною інформацією про розвиток ситуації і могло приймати рішення. За відсутності плану комунікації існує велика ймовірність того, що тривалість реагування збільшиться та/або команда

контактуватиме з особами, котрі не матимуть належних ресурсів для вирішення чи зменшення проблеми (Створення Команди реагування на інциденти кібербезпеки: початок роботи, 2006).

Зверніть увагу: також необхідно визначити, коли під час інциденту доцільно залучати правоохоронні органи, коли ні, через наслідки, які можуть позитивно чи негативно вплинути на вашу організацію.

4. Документація. Надзвичайно важливо наголосити, що цей елемент є особливо необхідним і може стати життєво важливим, коли справа доходить до реагування на інцидент. Найбільш вагомою причиною, чому слід обов'язково задокументувати інцидент, є те, що якщо даний інцидент буде визнано злочином, такий документ можна буде використати як доказ для притягнення підозрюваного (-них) до відповідальності через суд. Другою причиною є те, що документування є важливим для подальшого навчання команди. Це необхідно, щоб усі дії CIRT були задокументовані. Йдеться про усі вжиті заходи (наприклад, введені команди, системи, що постраждали, тощо) Документація повинна давати відповіді на запитання Хто, Що, Де, Чому і Як, якщо такі запитання колись виникнуть. Без такої інформації можна було б залишити відчуття невпевненості, якби щось поставило під сумнів, наприклад, форматування жорсткого диска та перевстановлення операційної системи на виробничому сервері (Newman, 2007).

   Порада: Чек листи із спеціальними колонками для нотаток, запису дат та часу та іншої відповідної інформації, можуть бути надзвичайно корисними особливо такі, у яких можна послідовно описати кожен крок реагування на інцидент.

5. Команда. CIRT слід створити з кількох людей, котрі є компетентними у різних дисциплінах, щоб вони могли впоратися з різними проблемами, що можуть виникати під час або внаслідок інциденту. Дехто з учасників цієї команди можуть бути адвокатами, спеціалістами з роботи з кадрами, з контактів з громадськістю, представниками IT персоналу різної спеціалізації і т.д. Дуже важливо повною мірою усвідомлювати, хто саме має входити до складу CIRT, тому що потреба у деяких спеціалістах та/або професіях може бути не настільки очевидною, як потреба у технічному персоналі для врегулювання інциденту (Реагування на порушення IT безпеки, 2011).

6. Контроль доступу. Іншим ключовим моментом є забезпечення того, щоб CIRT мала відповідні дозоли та права доступу, необхідні для виконання їхньої роботи. Прекрасним прикладом є підхід з системним адміністратором, який може давати або забирати дозволи до акаунтів учасників CIRT під час інциденту, щоб дозволити їм вирішити проблему, а після цього забрати права доступу, коли вони вже непотрібні (Реагування на порушення IT безпеки, 2011).

7. Інструменти. CIRT без інструментів - це як веслування на байдарках без весел, по суті важко щось зробити. Наполегливо рекомендуємо мати усе можливе програмне забезпечення та технічні засоби, які можуть бути легко використані під час інциденту. Сюди входить усе від антивірусів до лептопів з програмами для моніторингу пакетів даних, викруток та інших інструментів, а також чек листів для реагування на інцидент та інших речей, що можуть бути корисними (Бейтліх, 2005). Усі інструменти, що можуть знадобитися під час інциденту, повинні бути напоготові і у легкому доступі для CIRT під час інциденту.

8. Навчання. Це абсолютно необхідно, оскільки без навчання ваша команда буде погано підготовлена, і це призведе до повного провалу роботи над подоланням інциденту, навіть

незважаючи на найкраще планування. Рекомендується проводити відпрацювання через регулярні проміжки часу, щоб бути впевненим, що кожен учасник CIRT знає, як виконувати свої обов'язки під час інциденту.

ЩО ПОВИННА МАТИ НАПОГОТОВІ CIRT

- Журнал обліку спеціалістів, що працюють над подоланням інциденту, щоб задокументувати хто, як, де, чому і що зробив під час інциденту.
- Перелік контактів усіх учасників CIRT.
- Чисті USB накопичувачі.
- USB накопичувач або CD з сучасними засобами захисту від шкідливого програмного забезпечення та іншими програмними засобами, які можуть читати та/або записувати у файлові системи комп'ютерного середовища, у якому відбуватиметься реагування на інцидент. Прикладом може бути Bart's PE диск для операційної системи Windows XP (або пізніших).
- Ноутбук з програмами для розслідування інцидентів (наприклад, Autopsy, FTK or EnCase), антивірусними програмами та доступом до інтернету (на випадок, якщо буде потреба шукати інформацію, рішення або завантажувати інструменти).
- Набір інструментів для ремонту мереж та комп'ютера, щоб приєднувати/від'єднувати компоненти, мережеві дроти, кабелі і т.д.
- Жорсткі копіювальні пристрої з функціями запису та блокування, щоб створювати звукові копії зображень з жорсткого диску.
- Місце, у якій належить зберігати усе, перелічене вище, у відповідно організованих та захищених умовах.

ІДЕНТИФІКАЦІЯ

Ця фаза стосується встановлення та визначення величини відхилення від нормального функціонування в межах даної організації, до якого спричинився інцидент, а також його масштабу, з врахуванням того, що це відхилення і являє собою інцидент.

Зокрема для цього кроку потрібен спеціаліст, котрий збере інформацію про події з різних джерел, таких як системні журнали, повідомлення про помилки та інші ресурси. Такі системи встановлення факту втручання та брандмауери можуть надати дані для визначення того, чи є ця подія інцидентом.

Якщо певна подія визначається як інцидент, про неї слід якнайшвидше звітувати, щоб надати CIRT достатньо часу для збору фактів та підготовки запобіжних заходів (Бейтліх, 2005). На цьому етапі інциденту учасники

CIRT повинні бути повідомлені, і комунікація між ними і персоналом командного центру повинна бути налагоджена (наприклад, менеджмент та/або системні адміністратори).

Рекомендується задіяти принаймні двох учасників процесу, котрі здатні вирішити інцидент, таким чином один з них буде головним, котрий зможе приймати рішення по роботі з інцидентом, а другий допомагатиме збирати докази.

Комунікація та координація між учасниками CIRT (та менеджментом) є критично важливою, особливо якщо масштаби інциденту можуть мати значний вплив на функціонування бізнесу.

Цей етап також вимагає, щоб учасники команди реагування на інцидент занотовували усе, що вони роблять. Як і раніше, ці документи повинні відповідати на запитання Хто, Що, Де, Чому і Як, на той випадок, якщо документацію доведеться використати для переслідування у судовому порядку (Ньюман, 2007).

Після встановлення масштабів події та опису фактів, CIRT може перейти до наступного етапу (Реагування на інцидент, 2008)

Хорошим прикладом етапу ідентифікації є користувач, що контактує із службою технічної підтримки та звітує про те, що їхня система працює дивно або про те, що системи встановлення факту втручання повідомляють про незвичний трафік у мережі від певних хостів.

Це може розпочатися із якоїсь незвичної активності у системних логах, якої раніше ніколи не було. Надзвичайно важливо повною мірою усвідомлювати, наскільки величезною є множина можливих варіантів визначення інциденту.

Два інших приклади ще гіршої ситуації – це зникнення USB накопичувача або іншого пристрою для зберігання даних, та знаходження USB накопичувача користувачем у якомусь загальнодоступному місці, або кабелю, встромленого у комп'ютер, та запущеного процесу переписування даних, який має на меті крадіжку інформації або зараження систем.

СТРИМУВАННЯ

Основним завданням цього етапу є обмежити шкоду та запобігти подальшим пошкодженням від інциденту ("UF IT безпека," 2011). Цей етап складається з кількох кроків, однак, кожен з них є необхідним для повного стримування інциденту та запобігання знищенню будь-яких доказів, які можуть бути потрібні при подальшому зверненні до суду.

Першим кроком є короткотермінове стримування, тобто тут команда фокусується на тому, щоб зупинити пошкодження якнайшвидше.

Для короткострокового стримування можна ізолювати сегмент мережі від інфікованих робочих станцій або «покласти» виробничі сервери, які були атаковані і спрямувати весь трафік на резервні сервери. Короткострокове стримування не призначене для довгострокового вирішення проблеми; воно має на меті лише обмежити інцидент до того, як буде нанесено ще більше шкоди(Бейтліх, 2005).

Другий крок - резервне копіювання системи; перед видаленням або перенастроюванням системи необхідно зробити знімок ураженої системи за допомогою інструментів, добре відомих у спільноті комп'ютерної криміналістики, таких як Forensic Tool Kit (FTK), EnCase та ін. Це необхідне тому що, програмне забезпечення для розслідування інцидентів зафіксує пошкоджену систему (-ми) в такому стані, в якому вона перебувала під час інциденту, і тим самим збереже докази у випадку, якщо інцидент стався внаслідок злочинних дій або буде використовуватися для спостереження за тим, як система (-и) були скомпрометовані на етапі засвоєння уроків (Ньюмен, 2007).

Останній крок перед наступною фазою - це довгострокове стримування, що, по суті, є кроком, на якому пошкоджені системи можуть бути тимчасово полагоджені для того, щоб продовжувати

використовувати їх у виробництві, якщо це необхідно, під час відновлення систем на наступному етапі. Основна увага приділяється видаленню облікових записів та/або бекдорів, залишених зловмисниками на постраждалих системах, встановленню патчів як на пошкоджених, так і на сусідніх системах, а також обмеженню подальшої ескалації інциденту, одночасно дозволяючи продовжувати нормальні бізнес-процеси (Бейтліх, 2005).

Гарним прикладом стримування є від'єднання пошкоджених систем шляхом від'єднання мережевого кабелю або від'єднання їх від електромережі та знеструмлення вимикачів та/або роутерів, щоб ізолювати пошкоджені системи від тих, котрим нічого не загрожувало. Це, своєю чергою, ізолює проблему від усієї мережі та обмежить поширення будь-яких вірусів, або знизить ризик подальшого пошкодження системи.

ЛІКВІДАЦІЯ

На цьому етапі власне здійснюється повне видалення та відновлення пошкоджених систем. Як і на кожному попередньому етапі реагування на інцидент, тут буде необхідне продовження ведення ретельних записів щодо усіх вжитих заходів, щоб визначити вартість людино-годин та інших ресурсів, та подальшого визначення загальних наслідків ситуації для організації. Також необхідно переконатися, що вжито всіх потрібних заходів для видалення зловмисного та іншого забороненого контенту з усіх пошкоджених систем та для забезпечення повного їх очищення (Реагування на інциденти, 2008). Загалом це означатиме повторне форматування жорстких дисків системи, щоб переконатися, що увесь зловмисний вміст було видалено, та запобігти повторному зараженню. Це також етап, на якому захисні системи повинні бути покращені після вивчення того, що спричинило інцидент, та для забезпечення гарантії, що систему не буде пошкоджено таким чином знову (наприклад, встановлення захистів для усунення того типу вразливості, якою скористалися хакери і т.д.)

Гарним прикладом дій, що виконуються на етапі ліквідації, є використання оригінальних образів дисків, створених до розгортання системи у виробництві для відновлення системи, і подальше встановлення патчів та відключення невикористовуваних служб для того, аби захистити систему від подальших атак (наприклад, образ диску, створений з використанням програмного забезпечення). Також можна сканувати пошкоджені системи та/або файли з допомогою антивірусних програм, щоб переконатися, що приховані віруси теж видалено (тобто, використання антивірусних програм для знезараження систем та сканування реєстрів Windows на предмет наявності ключів, що можуть ініціювати запуск прихованого вірусу.

ВІДНОВЛЕННЯ

Метою цього етапу є обережне повернення уражених систем до робочого середовища таким чином, щоб це не призвело до нового інциденту. Надзвичайно важливо тестувати, відстежувати та підтверджувати, що системи, які повертаються до роботи, не були інфіковані вірусом повторно або пошкоджені якимсь іншим способом. На цьому етапі слід прийняти ряд важливих рішень, а саме:

- Щодо часу і дати повернення системи до роботи – життєво важливо, щоб остаточне рішення оператори/власники системи приймали на основі порад КРПК.

- Як тестувати і підтвердити, що пошкоджені системи є неінфікованими і справно працюють.

- Тривалість моніторингу на предмет наявності відхилень у роботі.

- Щодо інструментів для тестування, моніторингу та підтвердження справної роботи системи.

Можна перерахувати ще багато корисних рішень; однак вищенаведена інформація надає кілька основних ідей щодо цього етапу. Загальна основна мета, як було сказано раніше, - запобігти повторному інциденту, спричиненому тими самими проблемами, що спичинили й попередній (Реагування на порушення IT безпеки, 2011).

ЗАСВОЄНІ УРОКИ

Найбільш критичним етапом після усіх інших є етап Засвоєних уроків. Метою цього етапу є доповнення усієї документації, яке не було завершено під час інциденту, а також створення додаткової документації, яка може бути важливою при настанні майбутніх інцидентів. Також слід створити документ у формі звіту, який являтиме собою огляд усього інциденту. Цей звіт повинен відповідати на питання: Хто, Що, Де, Чому і Як, які можуть виникнути на зустрічі, присвяченій Засвоєним урокам. Головною метою є вивчити інцидент з моменту його виникнення в організації з метою покращення роботи команди, та надання матеріалів щодо інциденту.

Така документація також може бути використана як навчальні матеріали для нових учасників команди або як перелік певних стандартів для порівняння з діями під час майбутніх кризових ситуацій (Бейтліх, 2005). Слід провести зустрічі, присвячені засвоєним урокам якнайшвидше, бажано упродовж 2 тижнів після інциденту. Ці зустрічі також повинні бути записані у звіті про реагування на інцидент у формі резюме. Воно повинно бути коротким, щоб не втратити увагу аудиторії і залишитися на професійному рівні.

Гарним прикладом опрацювання Засвоєних уроків є формування переліку фактів щодо інциденту, які пояснюють наступні речі:

- Коли проблему було виявлено вперше і ким.

- Масштаби інциденту.

- Як інцидент було стримано та ліквідовано,

- Які роботи було здійснено під час етапу відновлення.

- У яких сферах CIRT були ефективними.

- Які сфери потребують покращення.

На цих зборах також слід виділити час на поради та обговорення між учасниками можливостей покращення роботи усієї команди. Цей етап є надзвичайно важливим, тому що тут учасники можуть обмінятися ідеями, щоб покращити роботу команди при настанні майбутніх інцидентів.

ЧЕК ЛИСТ ДЛЯ СПЕЦІАЛІСТІВ, ЩО ЗАЙМАЮТЬСЯ ПОДОЛАННЯМ ІНЦИДЕНТУ

ПІДГОТОВКА

1. Чи усі учасники повною мірою ознайомлені із політикою безпеки організації?

2. Чи усі учасники Команди реагування на комп'ютерні інциденти знають, з ким контактувати?

3. Чи усі учасники, що повинні реагувати на інцидент, мають доступ до реєстрів, а також доступ до усіх інструментів для здійснення актуального процесу протидії інциденту?

4. Чи усі учасники брали участь у навчанні на регулярних засадах для того, щоб відпрацювати процес реагування на інцидент на практиці та покращити загальний рівень професіоналізму?

ІДЕНТИФІКАЦІЯ

1. Де виник інцидент?

2. Хто звітував про те, що інцидент виявлено?

3. Як його було виявлено?

4. Чи є сфери, у яких після інциденту мають місце пошкодження? Якщо так, то які вони і коли їх було виявлено?

5. Які масштаби впливу?

6. Як це вплинуло на бізнес?

7. Чи було локалізовано джерело (-ла) інциденту? Якщо так, де і коли це було зроблено, а також якими є ці джерела?

СТРИМУВАННЯ

1. Короткотермінове стримування

    a. Чи можна ізолювати проблему?

        i. Якщо так, то слід перейти до ізоляції уражених систем.

        ii. Якщо ні, тоді слід працювати з власниками та/або менеджерами з метою визначення подальших дій, необхідних для стримування проблеми.

    b. Чи усі уражені системи ізольовані від неражених?

        i. Якщо так, то слід переходити до наступного кроку.

        ii. Якщо ні, тоді слід продовжувати заходи, спрямовані на ізолювання пошкоджених систем, доки фаза короткотермінового стримування не завершиться, і результатом не буде запобігання будь-якої подальшої ескалації інциденту.

c. Створення копії системи

i. Чи було створено копії пошкоджених систем для подальшого їх аналізу?

ii. Чи усі команди та іншу документацію було збережено від початку інциденту і донині?

- Якщо ні, слід задокументувати усі вжиті заходи якнайшвидше, щоб забезпечити наявність доказів на випадок звернення до суду та/або подальшого опрацювання Засвоєних уроків.

- Чи зберігаються копії, які можуть знадобитися у суді, у безпечному місці?
    - Якщо так, можна переходити до наступного кроку.
    - Якщо ні, слід помістити образ диску у безпечне місце для запобігання його пошкодженню та/або фальсифікації.

2. Довготермінове стримування

a. Якщо система може працювати офлайн, слід переходити до етапу Ліквідації.

b. Якщо система повинна залишатися активною, слід продовжити довготермінове стримування шляхом видалення усіх вірусів та інших шкідливих програм з уражених систем та захисту пошкоджених систем від подальших атак до настання ідеальних обставин, за яких стане можливою повторна інсталяція пошкоджених систем.

ЛІКВІДАЦІЯ

1. Якщо це можливо, слід повторно інсталювати систему і тоді встановити патчі та/або вжити інших заходів для запобігання або зменшення ризику атак.

a. Якщо ні, будь ласка, встановіть, чому?

2. Чи усі віруси та інші шкідливі програми, що залишили після себе хакери, було видалено, та чи було захищено пошкоджені системи від подальших атак?

a. Якщо ні, будь ласка, встановіть, чому?

ВІДНОВЛЕННЯ

1. Чи було захищено уражену систему від нещодавньої атаки, а також від можливих майбутніх?

2. Коли (дата і час) можна відновити пошкоджені системи для подальшої роботи?

3. Які інструменти ви збираєтесь використати для тестування, моніторингу та підтвердження того, що системи, які відновили свою роботу, не були знову пошкоджені тими ж засобами, які спричинили даний інцидент?

4. Як довго ви плануєте здійснювати додатковий моніторинг відновлених систем і що саме ви плануєте відстежувати?

5. Чи є якісь попередні показники, які можна використати в якості стандартів, щоб порівняти з ними результати моніторингу відновлених систем?

ЗАСВОЄНІ УРОКИ

1. Чи була написана вся необхідна документація щодо інциденту?

    a. Якщо так, слід згенерувати звіт про реагування на інцидент для проведення зборів, присвячених Засвоєним урокам.

    b. Якщо ні, слід зробити необхідні записи/створити документи якнайшвидше, поки нічого не втратилось для звіту.

2. Коли звіт про реагування на інцидент завершено, переконайтеся, що він відповідає на наступні питання щодо кожного етапу процедури реагування на інцидент: Хто? Що? Де? Чому? І Як?

3. Чи можна внести до розкладу заходів на наступні два тижні після вирішення інциденту зустрічі, присвячені Засвоєним урокам?

    a. Якщо ні, будь ласка, поясніть, чому, а також коли наступна найближча можливість провести ці зустрічі?

4. Зустрічі, присвячені Засвоєним урокам

    a. Розберіть процедуру реагування на тому інциденті, над яким працювали усі учасники CIRT.

    b. Чи обговорювались на зборах помилки або сфери, у яких процедуру реагування можна було б покращити?

i. Якщо такої дискусії не відбулося, будь ласка, поясніть, чому?