Досвід цивілізованих країн світу свідчить про те, що ефективна кібербезпека може бути досягнута лише шляхом комплексної реалізації правових, організаційних, технічних, наукових, навчальних заходів, ресурсного забезпечення для створення дієвої системи захисту кіберпростору в нашій державі.

Основними принципами діяльності у сфері кібербезпеки є:

координація заходів, що здійснюються для забезпечення кібербезпеки суб'єктами забезпечення кібербезпеки відповідно до їх призначення (специфіки діяльності) та повноважень;

взаємодія структур державного і приватного секторів на національному та міжнародному рівні з метою забезпечення адекватної відповіді кіберзагрозам;

пріоритетність завдань і зосередження зусиль на забезпеченні кібербезпеки об'єктів критичної інформаційної інфраструктури;

застосування новітніх технологій та передового досвіду для поліпшення стану кіберзахисту об'єктів критичної інформаційної інфраструктури. [3].

Отже, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки та оборони України. Протидія кіберзагрозам у сучасному безпековому середовищі повинна здійснюватися шляхом постійного посилення спроможностей національної системи кібербезпеки, використання цілісних та дієвих системних механізмів, адміністративно-правових методик та різноманітних засобів.

1. Щодо кібератаки на сайти військових структур та державних банків. Офіційний веб-сайт Кабінету Міністрів України. URL : https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-taderzhavnih-bankiv (дата звернення 27.02.2024).

2. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті Європейської інтеграції. URL : http://pag-journal.iei.od.ua/archives/2023/34-2023/14.pdf (дата звернення 27.02.2024).

3. Пфо О.М. Основні напрями забезпечення кібербезпеки України. URL : https://core.ac.uk/download/pdf/84825452.pdf (дата звернення 27.02.2024).

УДК 004.056.57
DOI: 10.31733/15-03-2024/2/331-332

Захар ДЕМИДОВ
старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі

Сергій КОЛОМІЙЦЕВ
науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі
Харківського національного
університету внутрішніх справ

СТРАТЕГІЯ РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ ТА КІБЕРІНЦИДЕНТИ

Умови війни завжди створюють серйозні виклики для кожної країни та суспільства. Загрози безпеці, економіці, інфраструктурі та громадському порядку можуть мати серйозні наслідки для населення. До них належать військові агресії, кібератаки, терористичні напади, масові збройні конфлікти та інші форми ворожості. Важливість запобігання, реагування та подолання наслідків воєнних загроз стає надзвичайно актуальною. Ретельний аналіз можливих загроз та їхнього впливу в умовах війни є важливим кроком у розробці ефективних стратегій захисту. Відповідно до цього, розробка стратегій для запобігання та ефективного реагування на надзвичайні ситуації є дуже важливою.

У різних організаціях реагування на кіберзагрози та кіберінциденти може проходити через різні етапи. Один з найбільш відомих циклів реагування на інциденти

розроблений Національним інститутом стандартів та технологій США (NIST). Цей цикл застосовується у різних галузях – від банківського сектору до військової та цивільної промисловості.

Сценарій реагування на інциденти – це попередньо визначений набір заходів для вирішення конкретних видів кіберінцидентів, таких як зараження шкідливим програмним забезпеченням, порушення політик безпеки або DDoS-атаки. Головною метою використання таких сценаріїв є можливість для швидкого та ефективного реагування на будь-які кіберзагрози з боку аналітичної команди. Сценарії реагування допомагають оптимізувати процеси в центрі моніторингу та реагування, що сприяє досягненню високого рівня зрілості в цій сфері.

Цикл складається з ряду фаз: підготовка, виявлення та аналіз, стримування, усунення та відновлення, пост-інцидентний аналіз. Всі ці етапи, визначені в NIST (або будь-яких інших процесах реагування на інциденти), можна поділити на конкретні блоки дій. Ці блоки можуть бути поєднані у різні сценарії залежно від характеру атаки для максимально швидкого та ефективного реагування. Кожна дія представляє собою просту інструкцію, яку виконує аналітик або автоматизований скрипт у разі інциденту.

Першою фазою в життєвому циклі реагування на інциденти за NIST є підготовка. Зазвичай це включає безліч етапів, таких як запобігання інцидентам (управління вразливістю, навчання користувачів, запобігання зараженню шкідливим програмним забезпеченням і т. д.). Перед початком реагування рекомендується визначити конкретні ролі кожного учасника у обробці різних типів інцидентів, а також розробити сценарії ескалації. Крім того, необхідно обрати інструменти для комунікації з учасниками процесу (наприклад, електронна пошта, телефон, месенджери або SMS). Команда реагування має мати відповідний рівень доступу до систем безпеки та IT-систем, програмного забезпечення та інтернет-ресурсів для форензики. Для оперативного реагування та уникнення помилок внаслідок людського фактора варто розробити механізми автоматизації та інтеграції, що запускаються системою управління засобами безпеки та автоматизації реагування на інциденти (SOAR).

Наступна важлива фаза – виявлення, що включає збір даних з IT-систем та засобів захисту, а також з загальнодоступних джерел і від людей в організації та поза її межами. Також визначаються передумови та ознаки атаки. Аналітик повинен переконатися, що отримані дані про інциденти відповідають умовам кореляційних правил, налаштованих для виявлення певних підозрілих змін. Основна частина фази аналізу – розслідування, що включає збір журналів, додаткової інформації про активи та артефакти, а також визначення області дії інциденту. Під час дослідження аналітик має зібрати всі дані про інцидент для визначення точки входу та «нульового пацієнта» – тобто того, як атаки отримали несанкціонований доступ і який хост або обліковий запис були скомпрометовані першими. Розширивши область аналізу відповідно до області дії інциденту, аналітик може отримати додаткову інформацію про активи та артефакти з джерел даних про загрози або локальних систем з інвентаризаційними даними, таких як Active Directory, IDM або CMDB. На останньому етапі аналізу команда реагування повідомляє про інцидент усіх зацікавлених осіб для забезпечення ефективного стримування загрози та відновлення.

Наступна значна частина життєвого циклу інциденту складається з фаз стримування, усунення та відновлення. Основна мета стримування – взяти ситуацію під контроль після інциденту та зменшити його наслідки. Команда повинна розуміти, які заходи стримування вживати в залежності від ступеня серйозності інциденту та потенційної шкоди. У фазі усунення з інфраструктури видаляються всі ознаки проникнення, такі як створені зловмисниками шкідливі файли, заплановані завдання та служби. Відновлення означає повернення системи до нормального режиму роботи. У цій фазі команді реагування слід провести перевірку працездатності системи і, за необхідності, відкотити зміни, зроблені під час атаки або реагування на неї. Остання фаза сценарію – пост-інцидентний аналіз, або робота над помилками. Основна мета у цій фазі – зрозуміти, як покращити процес реагування та запобігання подібним інцидентам у майбутньому.

Запобігання та реагування на будь-які серйозні загрози вимагає від уряду, військових та громадськості великих зусиль та координації. Швидке реагування та ефективне управління ризиками можуть допомогти зменшити наслідки воєнного конфлікту та зберегти життя та майно громадян.