Секція 1

ОЦІНКА РЕЗИЛЬЄНТНОСТІ ЦЕНТРІВ ОБРОБКИ ІНФОРМАЦІЇ

Кривенко Д. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Брежнєв Є. В.

Актуальність. Простій в роботі центру обробки даних (ЦОД) в декілька хвилин може призвести до фінансових та репутаційних втрат якщо, було допущено втрату даних своїх клієнтів. Тому постає питання забезпечення резильєнтності роботи ЦОД. На роботу таких центрів можуть впливати різні аварійні ситуації. Це можуть бути: кібератаки, несправність обладнання, програми з вимогою викупу, вимкнення електроенергії, стихійні лиха та навіть людські помилки. ІТ-команди з питань аварійного відновлення ЦОД мають розглянути всі можливі загрози і розробити плани дій щодо підвищення резильєнтності ЦОД.

Метою даної роботи є оцінка резильєнтності, як інтегрального показника захисту ЦОД.

Основні положення. Типовий ЦОД включає декілька технічних майданчиків які складаються з серверних шаф, мережевого обладнання, які забезпечують роботу ЦОД та його клієнтів. Завдання полягає в тому щоби забезпечити кібербезпеку ЦОД. Оцінювати рівень резильєнтності можна декількома способами.

Існує спосіб оцінки за допомогою відповідності до стандартів. Перевага способу в тому, що використовуватимуться методи сумісні між собою та добре налагоджені. Але є недоліки, метод не гнучкий, кібер загрози швидко адаптуються на відміну від стандартів які можуть швидко стати не актуальними. Потрібен великий час на оновлення стандартів та атестацію.

Другий метод заснований на математичних моделях. Математична функція може включати декілька показників - наприклад, частка втраченої інформації, інвестиції в захист інформації, їх рентабельність. Ці показники не однорідні між собою. та Не має загального методу вимірювання цих параметрів. Пошук рішення для захисту ускладнюється також тим, що протистояння в інформаційній сфері ведеться в умовах невизначеності, коли дії суперника невідомі і можуть бути передбачені лише з певною ймовірністю на основі статистичних даних або з допомогою експертної оцінки.

В якості показника резильєнтності пропонується використовувати параметр цільовий час відновлення (RTO). Він зосереджується на доступності сервісів та даних, враховує всі аспекти ІТ-інфраструктури, покладається на best practice в побудові відмовостійкої інфраструктури та моніторинг. За час встановленим RTO застосовані методи захисту повинні

виявити проблему, відреагувати та застосувати інструменти відновлення поки це не стане критичною втратою часу для роботи ЦОД.

Для визначення РТО пропонується застосувати систему моніторингу «Nagios». Це програма моніторингу комп'ютерних систем і мереж. Вона призначена для спостереження, контролю стану обчислювальних вузлів і служб, оповіщення адміністратора, якщо якісь із служб припиняють свою роботу.

Висновок. Резильєнтність – це інтегральний показник захисту ЦОД. Він враховує багато аспектів захисту, стійкості та можливості відновлення, які працюють в комплексі. Розглянутий ілюстративний приклад визначення РТО для типового ЦОД підтверджує можливість практичного застосування даного показника для задач визначення раціонального варіанту побудови систем захисту.

Список літератури

1. Effective Risk Management in the Data Center. *Datacenterknowledge*. URL – https://www.datacenterknowledge.com/archives/2017/05/08/effective-risk-management-data-center#close-modal (дата звернення: 26.09.2023);
2. Designing and Managing Data Centers for Resilience: Demand Response and Microgrids. U.S. Department of Energy;
3. What is data center resiliency and why is it important?. *Techtarget.* URL – https://www.techtarget.com/searchdatacenter/definition/resiliency (дата звернення: 06.10.2023).

Відомості про авторів

Кривенко Дмитро Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.kryvenko@student.csn.khai.edu

Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, старший науковий співробітник, e.brezhnev@csn.khai.edu