Секція 1

РОЗРОБКА І ДОСЛІДЖЕННЯ ІНТЕГРОВАНИХ СИСТЕМ БЕЗПЕКИ ЦЕНТРІВ З ОБРОБКИ ДАНИХ

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

Актуальність. Центр обробки даних (ЦОД) виконує функції обробки, зберігання і розповсюдження інформації, як правило, в інтересах корпоративних клієнтів – він орієнтований на вирішення бізнес-завдань шляхом надання інформаційних послуг. Консолідація обчислювальних ресурсів і засобів зберігання даних в ЦОД дозволяє скоротити сукупну вартість володіння IT- інфраструктурою шляхом можливості ефективного використання технічних засобів, наприклад, перерозподілу навантажень, а також шляхом скорочення витрат на адміністрування.

Сьогодні немає єдиного закону, який би регулював створення ЦОД і послуги, які вони надають за допомогою своєї інфраструктури, і вимоги до їхньої якості. Тож ми можемо виділити декілька проблемних питань з цього приводу, а саме технічний і програмний аспект та також правовий який повинен регулювати ці питання у взаєминах між постачальником послуг ЦОД та замовником. В технічному плані повинно бути забезпечена належна інфраструктура, комунікації та обладнання які забезпечують виконання завдання ЦОД, а також вирішення питань з безпеки як фізичної, функціональної, так і кібербезпеки.

Мета. Розглянути як сучасні компанії в Україні вирішують завдання з постачання послуг дата-центру, які їх особливості у вирішенні цього питання, також дослідити як забезпечуватися безпека, цілісність та доступність такої складної системи як ЦОД.

Основні положення. Отже оцінюючи можливі ризики що зустрічаюся в таких масивних системах можна виділити DDoS-атаки — надсилання великих обсягів фальшивого трафіку до комп'ютерної системи доти, доки обсяг трафіку не переповнить її, позбавивши доступу законних користувачів, встановлення шпигунського ПО, проникнення та викрадення інформації з носіїв або її псування, варто відмітити що проникнення може відбутися як зсередини так і ззовні, також проблеми доступу до інформації та її конфіденційність. Так також може відбутися фізичне втручання в роботу обладнання чи його знищення, різноманітні надзвичайні ситуації як відключення світла, повені, землетруси.

Вирішуючи питання ризиків було створено міжнародний стандарти такі як Uptime Institute та TIA-942, які регулюють ці питання. Мережа центру обробки даних вимагає повного аналізу нульової довіри, щоб бути включеною в будь-яку архітектуру ЦОД. Брандмауери центрів обробки

даних, засоби контролю доступу до даних, системи запобігання вторгненням (IPS), WAF і їхні сучасні аналоги системи захисту веб-додатків і API (WAAP) повинні бути належним чином розроблені, щоб гарантувати їхнє масштабування відповідно до потреб мереж центрів обробки даних. Крім того, вибираючи сховище даних або постачальника хмарних послуг, дуже важливо розуміти запобіжні заходи, які вони застосовують для свого власного ЦОД. Проведення аудитів безпеки. Це процес систематичного перевірки безпеки системи, включаючи перевірку наявності вразливостей. Він включає огляд конфігурацій, перевірку політик безпеки, перевірку прав доступу, аналіз журналів подій та інші процедури.

Висновки. До вирішення питань безпеки дата-центрів треба підходити комплексно, бо компоненти тісно пов'язані між собою. Обробка великого масиву даних компаніям потрібує забезпечення багатьох вимоги до інфраструктури, об'єму, захисту, цілісності та доступності інформації.

Список літератури

1. Юридичні основи роботи дата-центрів. *Mklegalservice.* URL – https://mklegalservice.com/tpost/4plhynlcg1-yuridichn-osnovi-roboti-data-tsentrv (дата звернення: 9.10.23);
2. С.В. Батечко, О.Ю. Лебедєва, В.В. Зоріло Методика оцінки захищеності інформаційних систем (2021). *Immm.* URL – http://immm.op.edu.ua/files/archive/n3_v11_2021/2021_3(3).pdf (дата звернення: 10.10.23);
3. TIA-942 Data Center Standards Overview. *TE Connectivity.* URL – http://www.te.com/content/dam/te/global/english/industries/enterprise-network-solutions/knowledge-center/documents/enterprise-white-paper-tia-942-data-center-standards-overview-102264ae.pdf (дата звернення: 10.10.23).

Відомості про авторів

Кривенко Дмитро Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.kryvenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, доцент, v.pevnev@csn.khai.edu