КІБЕРБЕЗПЕКА ХМАРНИХ ОБЧИСЛЕНЬ ТА БАЗ ДАННИХ

Тертичний В.О. Куценко Є. Є.
Науковий керівник – док.т.н. Шостко І.С.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

For any company, the most significant and valuable asset is data, since any possible data leakage can lead to the loss of critical important information, which will entail losses for the company. This means that its protection is one of the most difficult tasks facing the departments responsible for ensuring information security. The article describes methods for protecting cloud services and databases. Possible security threats in the area of cloud computing security and database protection were examined. It also considered recommendations for eliminating security threats in the field of cloud computing and also in the field of databases.

Захист баз даних є однією з найскладніших завдань, що стоять перед підрозділами, відповідають за забезпечення інформаційної безпеки. З одного боку, для роботи з базою необхідно надавати доступ до даних усім співробітникам, хто за службовим обов'язком повинен здійснювати збір, обробку, зберігання та передачу конфіденційних даних. Контроль і управління хмарами – є проблемою безпеки. Гарантій, що всі ресурси хмари пораховані і в ньому немає неконтрольованих віртуальних машин, не запущене зайвих процесів і не порушена взаємна конфігурація елементів хмари немає. Основні відомі загрози для хмарних обчислень: труднощі при переміщенні звичайних серверів в обчислювальній хмарі, динамічність віртуальних машин, уразливості всередині віртуального середовища, захист бездіяльних віртуальних машин, захист периметра і розмежування мережі

Для вирішення даних проблем компанією Cloud Security Alliance (CSA) були розроблені найбільш ефективні способи захисту в області безпеки хмар. До них відносяться такі методи як шифрування хмари яке є одним з найефективніших методів захисту даних. Провайдер, що надає доступ до даних повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також у випадку відсутності їх необхідності, безповоротно видаляти. Також провайдер для захисту даних при передачі повинен використовувати надійні протоколи такі як: AES, TLS, IPsec. Дані не вийде прочитати або зробити зміни, навіть у випадку доступу через ненадійні вузли. Також рекомендується використовувати аутентифікацію або ж для більшої надійності токени або сертифікати. Для прозорої взаємодії провайдера з системою індетіфікацію при авторизації, також рекомендується використовувати протоколи LDAP і SAML .

Також має сенс ізолювати користувачів використанням індивідуальної віртуальної машини і віртуальної мережі, які в свою чергу повинні бути розгорнуті з використанням таких технологій, як VPN, VLAN і VPLS.

Що стосується баз даних то існує кілька методів їх захисту. По-перше необхідно контролювати доступ до бази даних. Запобігти атаки кіберзлочинців допоможуть обмеження дозволів і привілеїв.

По-друге для компанії необхідно визначити критично важливі дані. Первим кроком має стати аналіз важливості захисту конкретної інформації.

Безумовно для запобігання витоку даних необхідно проводити моніторинг активності бази даних. Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як і ким. Однак найкращим способом захистити базу даних – зашифрувати її для осіб, які намагаються отримати доступ без авторизації. Для цього використовуються технології шифрування для перетворення інформації, что зберігається в базі даних, в шифротекст, що робить її прочитання неможливим для осіб, що не володіють ключами шифрування. Існує два основних способи шифрування інформації: симетричний та асиметричний. Асиметричне шифрування є більш безпечним, у порівнянні з симетричним, але в той же час воно істотно повільніше. Основні підходи можна класифікувати по тому, на якому рівні відбувається шифрування: на рівні сховища, на рівні бази даних, на рівні додатку.

На рівні сховища використовується так зване «прозоре» шифрування (англ. Transparent Database Encryption, TDE). Дані шифруються перед записом на диск і дешифруються під час читання в пам'ять, що вирішує проблему захисту «неактивних» даних, але не забезпечує збереження інформації при передачі по каналах зв'язку або під час використання.

Одним із прикладів шифрування на рівні бази даних є шифрування на рівні стовпців яке записує в базу даних вже зашифровані дані, а саму базу даних без подальшого шифрування в сховище.

У шифруванні на рівні додатків процес шифрування здійснюється додатком, яке створює або змінює дані, тобто він відбувається перед записом в базу даних.

Таким чином в доповіді запропоновані рекомендації щодо запобігання найбільш популярних атак на хмари і на бази даних, що дозволяє адаптувати запропоновані механізми захисту в будь-яку компанію.

Перелік посилань:

1. Загрози хмарних обчислень і методи їх захисту [Електронний ресурс].– Режим доступу до ресурсу: https://habr.com/ru/post/1831/ (дата звернення: 13.02.2020).

2. Захист баз даних – запорука безпеки корпоративної мережі Електронний ресурс]. – Режим доступу до ресурсу: https://eset.ua/ru/ blog/view/14/ (дата звернення: 13.02.2020)