УДК 004.056:355.451]:004.946

ІНФОРМАЦІЙНІ РИЗИКИ ПРИ РОБОТІ З ВІРТУАЛЬНИМ СЕРЕДОВИЩЕМ

Шульга М.Д.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківській національний університет радіоелектроніки, Харків, Україна
тел. (057) 702-13-20.

As the adoption of virtualization technologies grows, it attracts more attention from potential attackers. Issues such as data leaks, breaches in isolation, and insecure configurations can restrict flexibility and heighten risks linked to specific vulnerabilities. Identifying and addressing these risks help maintain the confidentiality, integrity, and availability of data in the virtual environment. Thus, early detection of information security risks bolsters risk management strategies.

Робота з віртуальним середовищем створює низку інформаційних ризиків, які організації повинні вирішити, щоб забезпечити безпеку та цілісність даних:

Вразливості гіпервізора, який керує віртуальними машинами, може стати мішенню для зловмисників. Таким чином одна з вразливостей може скомпрометувати все віртуальне середовище, це призведе до витоку даних або збоїв у роботі системи. Наприклад, дані що передаються між віртуальними машинами або через віртуальні мережі, можуть бути перехоплені, якщо вони не зашифровані або захищені належним чином.

Відсутність належної ізоляції між віртуальними машинами може призвести до несанкціонованого доступу або витоку даних між віртуальними машинами, порушуючи вимоги конфіденційності та безпеки.

Не відповідність конфігурацій компонентів віртуальної інфраструктури рекомендованим практикам, може наразити середовище на загрози безпеці, втрату даних або зниження продуктивності.

Внутрішні загрози: зловмисні інсайдери, які мають доступ до віртуального середовища, можуть навмисно чи ненавмисно спричинити витік даних, збої в роботі системи або інші інциденти безпеки. Неконтрольоване зростання віртуальних машин може довести до відсутності повного контролю над середовищем, ускладнюючи ефективне керування та охоплення захищеності всіх ресурсів. Нераціональне керування ресурсами може привести до проблем із продуктивністю або атак типу «відмова в обслуговуванні», що впливає на доступність критично важливих систем.

Неповне резервне копіювання або відсутність регулярного послідовного резервного копіювання віртуального середовища може привести до втрати даних, збоїв системи або тривалого процесу відновлення у разі збою або атаки.

Залежність технології віртуалізації від певного постачальника може обмежити гнучкість і збільшити ризики, пов'язані з вразливістю постачальника або обмеженнями підтримки з боку постачальника.

Організації повинні переконатися, що їх віртуальні середовища відповідають відповідним нормам, стандартам або вказівкам, таким як GDPR, або PCI DSS. Наприклад, згідно з GDPR, необхідно запровадження в компанії:

−реєстрів даних з ідентифікацією, які це дані, ким і для чого обробляються й кому передаються;

−призначення спеціального спеціаліста в компанії для дотримання заходів із поводженням із даними (Data Protection Officer), який повинен володіти знаннями в області права та досвідом із захисту даних [1].

Або сертифікат PCI DSS повинні мати будь-які торгово-сервісні компанії та постачальники послуг, що приймають, передають або зберігають дані міжнародних карт користувачів: основний номер карти (PAN), ім'я власника, термін дії та сервісний код. Серед них: банки, держустанови, e-commerce, розробники програмного забезпечення, хмарні оператори тощо.

В Україні отримання цього стандарту не регулюється законом. Але щороку з'являються IT-проекти: електронний та віртуальний банкінг, інтернет-магазини, а з введенням карантину почала активно розвиватися онлайн-торгівля. Питання забезпечення кібербезпеки для них є найбільш важливим, адже це, в першу чергу, питання репутації та статусу на ринку. Компанії, які не мають цього сертифікату, можуть погано захищати дані клієнтів. Тому стають легкою мішенню для шахраїв, і компенсувати збитки клієнтам в разі інциденту доведеться саме їм [2].

Усунення інформаційних ризиків під час роботи з віртуальним середовищем вимагає комплексного підходу, який включає впровадження надійних засобів контролю безпеки, регулярний моніторинг і сильну стратегію управління ризиками.

Список використаних джерел:

1. GDPR для юристів, або як підготуватися до неминучих змін. https://yur-gazeta.com/dumka-eksperta/gdpr-dlya-yuristiv-abo-yak-pidgotuvatisya-do-neminuchih-zmin-.html

2. Як хмара допомагає отримати сертифікат PCI DSS. https://gigacloud.ua/blog/navchannja/jak-hmara-dopomagae-otrimati-sertifikat-pci-dss