УДК 004.056:355.451]:004.946

ОЦІНКА ІНФОРМАЦІЙНИХ РИЗИКІВ 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

During an information security audit, a fair evaluation of the virtual environment's data protection level is conducted. The audit results reveal the effectiveness of information security and access control measures within the virtual setting, as well as ways to minimize risks when handling confidential information. Evaluating information security risks and employing a holistic risk management approach in a virtual environment enables organizations to better safeguard their virtual infrastructure, maintain data security, and uphold the integrity of their IT systems. By adopting a proactive stance, companies can stay ahead of emerging threats and adjust to evolving developments in the virtualization landscape.

Оцінка інформаційних ризиків під час роботи з віртуальним середовищем має вирішальне значення для підтримки безпеки та цілісності даних та IT-ресурсів. Нижче представлено ключові кроки для оцінки ризиків віртуальної інфраструктури.

Необхідно здійснювати каталогізацію всіх активів у віртуальному середовищі, включаючи віртуальні машини, гіпервізори, мережі та системи зберігання.

Проводити оцінку потенційних загроз, наприклад, зловмисне програмне забезпечення, несанкціонований доступ, витік даних і внутрішні загрози, які можуть вплинути на віртуальне середовище.

Пропонується систематично проводити регулярну оцінку вразливостей, включаючи сканування та пентест, щоб визначити пріоритети для закриття слабких місць у віртуальній інфраструктурі.

Необхідно проводити оцінку імовірності та потенційного впливу кожної виявленої загрози та вразливості, враховуючи такі фактори, як вартість активів, використані засоби контролю безпеки та потенційні наслідки атаки.

Здійснювати процедури ранжування ризиків на основі їх впливу та ймовірності реалізації, зосереджуючись на розгляді найбільш критичних даних.

Пропонується розробити та запровадити засоби контролю безпеки. Це може включати контроль доступу до даних, шифрування, моніторинг та резервне копіювання іміджів.

Робити перевірку віртуального середовища на наявність несанкціонованих подій та інцидентів у сфері безпеки. Необхідно оновлювати підходи до оцінки ризиків, це необхідно, щоб врахувати зміни в середовищі, оцінити нові загрози або виправити реалізацію організаційних вимог для доступу к даним.

Пропонується проводити безперервне підвищення обізнаності та навчання для співробітників, щоб зменшити ймовірність людських помилок або внутрішніх загроз, гарантуючи, що вони ознайомлені з найкращими практиками та можливими ризиками, пов'язаними з віртуальним середовищем.

Розробити та підтримувати плани реагування на інциденти та безперервності бізнесу, щоб забезпечити швидке аварійне відновлення системи та мінімізувати вплив інцидентів безпеки.

Необхідно провести оцінку безпеки постачальників технологій чи послуг віртуалізації. Оцінити методи безпеки та відповідність галузевим стандартам і правилам [1].

Проводити звітування про виявлені ризики, стратегії пом'якшення та їх вплив на організацію відповідним зацікавленим сторонам, зокрема керівництву, IT-командам і співробітникам.

Також необхідно проводити регулярні оцінки ризиків, щоб виявити нові ризики або ризики, що розвиваються, оцінити ефективність існуючих засобів контролю та за потреби скоригувати стратегію управління ризиками.

Вести повну документацію щодо оцінки ризиків, засобів контролю безпеки та планів реагування на інциденти.

Зберігати записи про події безпеки, інциденти та зміни у віртуальному середовищі, щоб полегшити майбутні оцінки ризиків і перевірки.

Сприяти розвитку культури безперервного вдосконалення, навчання на інцидентах і адаптації стратегії управління ризиками для вирішення нових загроз, вразливостей та змін у цілях або вимогах організації.

Список використаних джерел:

1. Білецький Е. В., Янушкевич Д. А., Шайхлісламов З. Р.. (2015). Управління якістю продукції та послуг