УДК 004.056:004.946

МЕХАНІЗМИ ЗАХИСТУ ВІРТУАЛЬНОГО СЕРЕДОВИЩА

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 continues to expand, so do the threats to information security, leading to heightened focus on protective measures. Virtual infrastructure is becoming increasingly reliable and capable of addressing a broad spectrum of security issues. However, the primary challenges concerning virtualization platform security lie in the design of the final solutions based on them. It is evident that deploying a virtual infrastructure presents distinct security challenges, such as hypervisor vulnerabilities, virtual machine (VM) isolation, and configuration errors. Identifying and mitigating these risks contribute to preserving the confidentiality, integrity, and availability of an organization's data and IT resources.

Метою управління ризиками IT-проектів є оперативне виявлення факторів, пов’язаних з виконанням інформаційної системи або системи автоматизації, які можуть негативно вплинути на реалізацію проекту, та оптимальне планування дій для мінімізації цих факторів.

Сьогодні багато організацій покладаються на віртуальне середовище як на критичне програмне забезпечення для тестування рішень. Забезпечення захисту даних віртуального середовища є важливим компонентом корпоративної інформаційної безпеки протягом багатьох років розгортання віртуальної інфраструктури. Робота з віртуальними машинами пов'язана з різними ризиками. Механізми захисту у віртуальному середовищі необхідні для забезпечення безпеки та цілісності віртуалізованих систем. Для захисту віртуальної інфраструктури можна використовувати різні методи.

Безпека гіпервізора. Перевіряти чи встановлені останні оновлення ОС, налаштування віртуальних машин відповідають політикам організації, це знизить ризик використання вразливостей.

Ізоляція віртуальної машини. Використання політики ізоляції віртуального середовища, наприклад, ізольованої мережі для тестування рішень з налаштованими брандмауерами, щоб запобігти можливому витоку даних або несанкціонованому доступу.

Безпека мережі. Використання брандмауерів, системи виявлення та запобігання вторгненням (IDPS) і сегментацію мережі для захисту мережевого трафіку віртуального середовища.

Контроль доступу. Реалізація механізмів автентифікації та авторизації для керування доступом до віртуальних ресурсів. Використання

багатофакторної автентифікації (MFA), щоб обмежити доступ до конфіденційної інформації та ресурсів.

Шифрування. Використання шифрування носіїв такими утилітами як Bitlocker, McAfee Drive Encryption.

Моніторинг і аудит безпеки. Необхідно систематично робити аудит віртуального середовища для виявлення потенційних загроз, вразливостей або неправильних налаштувань. Можливе впровадження системи керування журналами та інформацією про безпеку та керування подіями (SIEM), щоб збирати й аналізувати події безпеки.

Керування виправленнями. Проводити оновлення ОС віртуальних машини та програмного забезпечення за допомогою патчів та оновлень безпеки.

Резервне копіювання та аварійне відновлення. Необхідно створити правила резервного копіювання даних і конфігурацій, а також створення іміджів систем для аварійного відновлення, щоб забезпечити доступність і цілісність віртуального середовища у разі збоїв або атак.

Безпечна конфігурація. Необхідно дотримуватись найкращих рекомендацій і практик щодо безпечного налаштування компонентів віртуальної інфраструктури, таких як гіпервізори, віртуальні машини та пристрої віртуальної мережі.

Безпека кінцевих точок. Використовувати антивірусне програмне забезпечення, систему захисту від зловмисного програмного забезпечення та системи запобігання вторгнень на основі хосту (HIPS).

Проводження навчання. Проводити навчання співробітників можливим проблемам безпеки та найкращим практикам, пов'язаним із віртуальними середовищами, це зменшить ймовірність людських помилок або внутрішніх загроз.

Список використаних джерел:

1. Що таке багатофакторна автентифікація та коли доцільно її використовуватиTechnologies. https://yubikey.com.ua/shcho-take-bahatofaktorna-avtentyfikatsiia-ta-koly-dotsilno-ii-vykorystovuvaty

2. Система виявлення вторгнень (HIPS). https://help.eset.com/ees/7/uk-UA/idh_hips_main.html