УДК 004.8+65.05+681.5
DOI: 10.31673/2412-9070.2019.051926

Ю. І. КАТКОВ, канд. техн. наук, доцент;
Ю. В. БЕРЕЗОВСЬКА, аспірант;
М. М. РИЖАКОВ, аспірант;
Д. С. ГНИДЮК, студент.
Державний університет телекомунікацій, Київ

АНАЛІЗ РИЗИКІВ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ І КОНТЕЙНЕРИЗАЦІЇ В ХМАРНИХ СЕРВІСАХ

У статті розглядається проблема наслідків застосування технологій віртуалізації і контейнеризації в хмарних сервісах. Застосування віртуалізованої ІТ-інфраструктури надає бізнесу масу переваг, а саме: дозволяє скоротити витрати, спростити експлуатацію серверів і клієнтських пристроїв. Однак одночасно виникають нові загрози для безпеки даних і мереж, відбувається збільшення інформаційних ризиків і створюються умови для компрометації віртуальних машин. Тому рішення щодо забезпечення захисту віртуалізованої ІТ-інфраструктури перестали бути виключно технічними, тепер вони охоплюють організаційні заходи і передбачають практичні заходи щодо усунення проблемних ситуацій. Причина збільшення інформаційних ризиків закладено в самій природі віртуалізації. Причина в тому, що віртуальна інфраструктура відрізняється від фізичної двома елементами: гіпервізором і засобом управління гіпервізором. Гипервізор і засіб управління нім є критичними елементами віртуальної ІТ-інфраструктури. Вони створюють загрози для віртуалізації ІТ-інфраструктури. Описано особливості цих загроз при впровадженні віртуалізації і контейнеризації в хмарних сервісах. Показано, що найбільша небезпека для віртуалізованої ІТ-інфраструктури криється в тому, що слабкі місця у вирішеннях для віртуалізації дозволяють зловмисникові впливати за допомогою шкідливого коду на гипервізор хостової операційної системи, тому створюються умови впливу на гостьові системи. Якщо зловмисник отримає повний контроль над гіпервізором, йому стануть доступні всі підімкнені розділи мережі, масові системи зберігання і всі віртуальні машини. Розглядаються найбільш імовірні загрози для віртуалізованої ІТ-інфраструктури, а саме: загроза безконтрольної маніпуляції з віртуальними машинами; загроза для консолідації віртуальних машин; загроза уразливості платформ віртуалізації. Запропоновано організаційні заходи забезпечення захисту віртуалізованої ІТ-інфраструктури шляхом зміцнення гипервізора і розробки мережної концепції. Розглянуто інструменти захисту віртуалізованої ІТ-інфраструктури.

Ключові слова: віртуалізація; контейнеризація; загроза; уразливість; ІТ-інфраструктура.

Вступ

Віртуалізація — це процес створення програмного (або віртуального) уявлення чого-небудь, наприклад віртуальних додатків, серверів, сховищ і мереж. Віртуалізація в інформаційних технологіях (ІТ) — процес подання набору обчислювальних ресурсів або сутностей, який дає певні переваги перед оригінальною конфігурацією [1]. Віртуалізація — це єдиний і найефективніший спосіб скорочення витрат на ІТ-інфраструктуру при одночасному підвищенні ефективності та адаптивності для компаній будь-яких розмірів. ***Контейнери*** — це новий рівень віртуалізації ІТ-інфраструктури. Вони ізолюють окремі процеси всередині однієї операційної системи (ОС) і запускають їх із загальним доступом до бібліотек та ресурсів цієї ОС. Завдяки контейнерам кожний окремо запущений додаток зберігає всі переваги хмари: резервованість, безперебійність роботи, масштабованість, автоматичне керування. Тому технології віртуалізації набувають все більшої популярності. Великі компанії віртуалізують свої локальні сервери і будують приватні «хмари», малий і середній бізнес активно користується хмарними сервісами і орендує ресурси в ЦОДах. Тому стає зрозумілим, що створення віртуалізованої ІТ-інфраструктури дозволяє скоротити витрати, спростити експлуатацію серверів і клієнтських пристроїв, проте одночасно виникають нові загрози для безпеки даних і мереж. Вирішення щодо забезпечення захисту таких платформ перестали бути виключно технічними, тепер в них включаються організаційні заходи і передбачаються практичні заходи щодо усунення проблемних ситуацій [2]. Таким чином, застосування віртуалізованої ІТ-інфраструктури приносить бізнесу не тільки масу переваг, а й існує і зворотний бік — збільшення інформаційних ризиків та компрометація віртуальних машин з боку управління інфраструктурою.

Причину збільшення інформаційних ризиків закладено в самій природі віртуалізації. Йдеться про те, що віртуальна інфраструктура відрізняється від фізичної двома елементами: гіпервізором і засобом управління цим гіпервізором. Гіпервізор є прошарком між апаратною і програмною частиною, яка виконує віртуальні машини, а засіб управління є інструментом, що дозволяє централізовано керувати гіпервізорами. Звідси стає зро-

зумілим, що при компрометації гіпервізора будуть скомпрометовані і віртуальні машини, які створені ним. Якщо скомпрометовано засіб управління, то і вся інфраструктура знаходиться під загрозою. Таким чином, гіпервізор і засіб управління ним є критичними елементами віртуальної інфраструктури. Вони створюють загрози для віртуалізації IT-інфраструктури.

Найбільш типові ризики стосовно віртуалізації IT-інфраструктури (віртуалізації серверів) пов'язані [2] з неможливістю застосування традиційних засобів для захисту віртуальної інфраструктури; з консолідацією додатків та інформації різних рівнів значимості на одному фізичному сервері без забезпечення їх достатньою ізоляцією; з відсутністю інструментів контролю адміністраторів віртуальної інфраструктури; з уразливими і недокументованими можливостями в платформі віртуалізації. Треба враховувати, що не викликає сумнівів теза про меншу захищеність віртуального аналога порівняно з фізичним комп'ютером. Досить порівняти надійність ізоляції віртуальних машин з варіантом фізично ізольованих комп'ютерів. Навіть у нових технологіях апаратної віртуалізації частина механізму віртуалізації реалізується програмним забезпеченням гіпервізора. Незважаючи на оптимізацію обсягу коду гіпервізора і пильну увагу розробників до усунення можливих вразливості, існує ненульова ймовірність наявності прихованої або функціональної уразливостей гіпервізора і можливості проведення проти нього атаки. Це знижує захищеність і простоту переспрямування віртуальних систем на інші фізичні платформи, використання віртуальних машин в архітектурі «хмарних обчислень». Таким чином, це завдання є актуальнім та своєчасним.

Постановка завдання. Стає наочним, що віртуалізація IT-інфраструктури надаючи нові можливості, сприяє появі певних факторів ризику для віртуальної інфраструктури. Виникає актуальне завдання щодо визначення способів захисту технологій віртуалізації IT-інфраструктури.

Аналіз останніх досліджень і публікацій. Віртуалізація породжує не тільки переваги, а й ризики для IT-інфраструктури, тому необхідно спеціальні засоби, що захищають віртуалізацію [1]. Вирішення цього завдання щодо захисту віртуалізації IT-інфраструктури почалося кілька років тому (2012 р.) і триває досі [2]. Одним із перших свої рекомендації щодо захисту технологій віртуалізації видав Національний інститут стандартів і технологій США (NIST). Зараз міжнародна організація Cloud Security Alliance випустила вже третю редакцію керівництва з безпеки хмарних середовищ. У цих документах, зокрема, дано перелік заходів захисту, обов'язкових при використанні віртуальних середовищ у державних інформаційних системах та інформаційних системах персональних даних. При цьому особливу увагу приділено необхідності застосування сертифікованих засобів захисту віртуального середовища. Засоби захисту віртуального середовища спрямовано на створення інструментів контролю і протидії зловмисникам або зловживанням [5; 6]. Таким чином, формуються умови щодо визначення дій, які необхідно виконати для зниження інформаційних ризиків і забезпечення безпеки застосування технологій віртуалізації IT-інфраструктури.

Основна частина

Розв'язування питання як впливають технології віртуалізації на інформаційну безпеку (ІБ) IT-інфраструктури (підвищується, знижується або залишається на колишньому рівні) вимагає розгляду існування різних видів віртуалізації.

Віртуалізація комп'ютера. Віртуалізація комп'ютера — найбільш поширений вид віртуалізації. Існують технології програмної і апаратної віртуалізації. Програмна віртуалізація має низку особливостей, що створюють серйозні проблеми ІБ: гіпервізор і хостова ОС представляють єдину точку відмови; реалізація гіпервізора у вигляді програмного модуля більш вразлива до атак, ніж апаратно-програмна реалізація; відомі вирішення щодо програмної віртуалізації не забезпечені захистом на апаратному рівні за технологією апаратної віртуалізації TPM (*Trusted platform module*). Більш сучасна технологія апаратної віртуалізації вирішує ряд зазначених проблем ІБ. Для підвищення захищеності компанія Intel упровадила в одному зі своїх чіпсетів технологію безпеки LaGrande/TXT, що використовує специфікацію TPM 1.2. Дана технологія дозволяє контролювати цілісність програмно-апаратної середовища комп'ютера. Аналогічні механізми безпеки забезпечує технологія AMD-V, в якій реалізовано спеціальний захищений режим запуску монітора віртуальних машин.

Віртуалізація мереж. Віртуалізація мереж являє собою перетворення елементарних мережних ресурсів типу фрейму, пакета, сесії і управління ними. При цьому можуть використовуватися канальний, мережний, транспортний і сесійний рівні моделі OSI. Віртуалізація мереж можлива за технологією віртуальної приватної мережі (VPN — *Virtual Private Network*) і за технологією віртуальної локальної обчислювальної мережі (VLAN — *Virtual Local Area Network*). VPN має глобальний характер застосування, оскільки працює на мережному рівні, у VLAN — тільки локальний. Основними цілями віртуалізації мереж є: поділ і управління потоками інформації, мережна ізоляція, сегментування мережі, а також захист інформації при її передаванні по мережі.

Віртуалізація додатків. При розгляді віртуалізації додатків треба розрізняти віртуалізацію додатків (робота з контекстами) і віртуалізацію уявлень (робота протягом термінальної сесії, визначення профілю користувачів). Віртуалізація додатків ставить собі за мету: відокремити додатки від ОС, зробити їх мобільними і надати можливість для виконання додатків у різних середовищах. Віртуалізація уявлення — це підхід, при якому додаток виконується на віддаленому сервері, а його користувальницький інтерфейс відображається локально. Віртуалізація уявлення широко використовується в сучасних додатках для управління клієнтськими додатками і захисту конфіденційних даних. Віртуалізація уявлень за допомогою термінальної сесії — хороший метод ізоляції сервера додатку і робочої станції користувача. Ізоляція користувача і сервера важлива при їх локалізації в двох зонах, протилежних за умовами ІБ. При термінальній сесії на сервер передаються тільки коди натиснутих клавіш робочої станції, а з сервера — растри призначеного для користувача інтерфейсу. Важливо, що між сервером і робочою станцією немає обміну програмним кодом, що виключає ризик передавання шкідливих програм.

Застосування віртуалізації в задачах ІБ. Віртуалізація мереж на базі загальноприйнятих протоколів IP Security (IPSec), захищених сокетів Secure Sockets Layer (SSL) і приватних протоколів Virtual Private Network (VPN) — є самостійним напрямком мережної безпеки.

Застосування апаратної віртуалізації. Сьогодні ізоляцію даних і процесів між віртуальними машинами забезпечують нові продукти компаній IBM, Intel, Microsoft, AMD, Citrix (Zen), VMware. Гарантована ізоляція дозволяє їх застосування для розділення операційних середовищ за рівнем конфіденційності інформації, що обробляється в системі. Технологія апаратної віртуалізації, що використовує модуль Trusted platform module (TPM), який виконує функції безпеки (наприклад, BitLocker або DDPE), і в специфікації адресно-часової — код Time Code Generator (TCG), для реалізації довірчого середовища, дозволяє створювати безпечні розділи з перевіркою ідентичності і цілісності віртуальної машини і всіх задіяних у ній програмно-апаратних компонент. Поки тільки компанії Parallels і Microsoft поставляють на ринок продукти віртуалізації, що застосовують ці технології захисту. Компанія Parallels працює над використанням Intel VT-x і TXT для створення монітора віртуальних машин із гарантованим захистом від вірусів. Компанія Microsoft використовує технологію апаратного захисту в рамках Windows Server 2008 і Hyper-V Server. Концентрація кількох віртуальних машин на одному апаратному пристрої підвищує складність конфігурації. При інтеграції в існуюче мережне середовище гіпервізор охоплює безліч зон, що дозволяє надавати послуги в різних точках мережі. При цьому можливе перекриття з класичними системами мережної безпеки. Але оновлення вимагається частіше, а це погіршують ситуацію.

Існування різних видів віртуалізації передбачає наявність таких загроз [6]: обмін файлами між Хостами і Гостями; зображення і знімки містять конфіденційні дані; інструменти сніффінга мережного зберігання; конфігурація; гіпервізор має вбудований контроль доступу, а віртуалізація хоста (гипервізор розміщено на фізичній ОС сервера) — не має; втрата даних віртуальних машин еквівалентна проникненню в дата-центр та ін. Також існують деякі категорії атак, типові для віртуалізації: відмова від обслуговування (DoS); неконтрольоване переміщення між віртуальними машинами; перехоплення трафіку хоста. Розглянемо ці загрози[6].

Загроза від обміну файлами між хостами і гостями. У разі спільного використання файлів, зламаний гість може отримати доступ до вузла файлової системи і змінити каталоги, які використовуються для обміну інформацією. Стає зрозумілим, що загальний доступ до буфера обміну використовуються і гостем, і хостом, або коли для програмування використовується API, істотні помилки в цих областях можуть поставити під загрозу всю інфраструктуру.

Загроза від втрати зображення або знімків, що містять конфіденційні дані. Зображення і знімки містять конфіденційні дані, такі як особисті дані і паролі, у тому самому вигляді, як ці дані зберігаються на фізичному жорсткому диску. Будь-які непотрібні або додаткові зображення можуть дійсно заподіяти проблеми. Усі знімки, які були збережені з шкідливими програмами, у майбутньому можуть бути перезавантаженими і стати причиною хаосу. Крім того, якщо змінюється політика безпеки, то є доступ до певних функцій. Звідси журнал аудиту може бути втраченим, що виключає запис змін, які можливо зробили на сервері. Це може спричинити складності. Звідси стає зрозумілим, що якщо не буде моментальних знімків, будь-які зміни конфігурації будуть втрачені.

Загроза від сніффінга. Сніффер (sniff) — це аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів. Інструменти сніффінга можуть використовуватися для читання або запису даних системи зберігання і це може бути використано для перезбірки для зручності зломщика в майбутньому. Наприклад, є оптоволоконний канал із протоколом iSCSI (*Internet Small Computer System Interface* — прото-

кол, який базується на TCP/IP і розроблений для встановлення взаємодії та управління системами зберігання даних, серверами і клієнтами). Він є чітким текстовим протоколом і може бути уразливим для атак типу «людина посередині», тобто тип інтернет-атак, при яких зловмисник перехоплює канал зв'язку, отримуючи повний доступ до інформації, що передається.

Загрози через гіпервізор. Перша загроза від гіпервізора у тому, що якщо гіпервізор знаходиться під загрозою, то також будуть під загрозою і всі під'єднані до нього віртуальні машини, а конфігурація гіпервізора за замовчуванням не завжди є найнадійнішою. Проблема у тому, що гіпервізор керує всім і забезпечує єдину точку збою у віртуальному середовищі. Будь-яке порушення може поставити під загрозу все віртуальне середовище. Це пов'язане з тим, що голе залізо гіпервізора зазвичай має вбудований контроль доступу, а віртуалізація хоста (гіпервізор поміститься на фізичній ОС сервера) не має. Віртуалізація хоста піддає систему великим загрозам через наявність гіпервізора в ОС.

Друга загроза від гіпервізора це те, що адміністратор може зробити все що завгодно на гіпервізорі (у нього є «ключі від усіх дверей»). Дії на гіпервізор зазвичай захищені паролем, але пароль можна легко передати і повністю відмінити. Отже, ніколи не можна дізнатися, який із адміністраторів виконав певну дію.

Наступна загроза від гіпервізора це те, що гіпервізор дозволяє віртуальній машині зв'язуватися одна з одною, і така взаємодія навіть не переходить до фізичної мережі. Це діє як приватна мережа для віртуальних машин. Такий трафік не завжди можна побачити, оскільки він виконується гіпервізором, і не можна захистити те, про існування чого не знаєте.

Загрози від віртуальній машини. Загрози від віртуальній машини (ВМ) такі:

- ВМ можуть масштабуватися, їх просто скопіювати на віддалений комп'ютер або портативний пристрій зберігання даних. Втрата даних на ВМ буде еквівалентна проникненню в дата-центр, минаючи фізичну безпеку, і злодійства фізичного сервера.
- ВМ, що встановлені користувачами, не завжди відповідають політиці безпеки організації і можуть не мати будь-якого встановленого програмного забезпечення для безпеки.
- ВМ, що тільки-но створені, зазвичай мають відкриті порти і безліч доступних протоколів.
- Кожного разу при створенні ВМ, додається інша ОС, яку необхідно захищати, патчити, оновлювати і підтримувати. Додаткова ОС з проблемами може збільшити загальний ризик.
- Неактивні ВМ (у тому числі ВМ, які більше не використовуються) все ще можуть містити важливі дані — такі, як дані верифікації та інформацію про конфігурацію.
- Будь-яка функціональність буфера обміну, що дозволяє ділитися даними між ВМ і хостом, може стати точкою проникнення для шкідливих програм, які потім будуть перенесені на ВМ.
- Не ізольовані ВМ можуть мати повний доступ до ресурсів хоста. Тому злом ВМ може призвести до злому всіх ресурсів.
- ВМ можуть бути створені користувачами без повідомлення ІТ-відділу організації. Якщо ці ВМ не помітили, то вони і не будуть захищені.
- Зараження ВМ може призвести до зараження сховища даних, а інші ВМ можуть використовувати ці самі сховища.
- ВМ можуть збільшувати потреби у ресурсах дуже швидко, і це може викликати напруженість в системах безпеки. Якщо вони не будуть ефективно автоматизовані, то буде збільшуватись навантаження на адміністратора в зв'язку з необхідністю установки оновлень, виправлень та ін., що зумовить помилки типу «людський фактор».
- Заражені ВМ можуть з'явитися непомітно і заразити інші ВМ, а потім зникнути перш ніж їх помітили.

Загрози від нераціонального поділу обов'язків і права доступу адміністратора.

- У звичайних фізичних мережах адміністратори сервера займаються управлінням серверами, в той час як адміністратори мережі управляють мережами. Персонал служби безпеки зазвичай співпрацює з обома групами адміністраторів. У віртуальних середовищах, управління сервером і мережею може відбуватися на єдиній консолі управління і це ставить нові завдання для ефективного поділу обов'язків.
- Системи віртуалізації дають повний доступ до всіх дій віртуальної інфраструктури. Це, як правило, замовчується, тому не завжди змінюються і злом доступу адміністратора може забезпечити повний контроль над віртуальною інфраструктурою.

Загроза від синхронізації часу. Годинники кожної віртуальної машини повинні бути єдиними, але, коли це поєднується зі зміщенням показань звичайного годинника (помилками в часі), завдання можуть виконуватися занадто рано або пізно, що може призвести до плутанини в логах і втрати точності даних. Неправильне відстеження часу надаватиме недостатньо даних для будь-яких майбутніх розслідувань.

Загрози від мережі VLAN.

- Використання VLAN вимагає маршрутизації трафіку ВМ, наприклад, з хоста до брандмауера. Це може призвести до затримок між пристроями мережі, що в подальшому призведе до проблем з продуктивністю.

• Комунікація всередині ВМ не захищена і не досліджується на VLAN. Також, якщо на одному і тому самому VLAN знаходяться кілька ВМ, поширення шкідливих програм з однієї віртуальної машини на іншу не можна зупинити.

Загроза від розділів під час запуску на одному хості кількох віртуальних машин. Вважається, що коли на одному хості запущено кілька віртуальних машин, вони ізольовані одна від одної і одна ВМ не може бути використана для атаки на іншу. Технічно, ВМ можна розділити, але розділи на одній ВМ ділять ресурси пам'яті, процесора і пропускну здатність. Якщо певний розділ споживає занадто багато одного із зазначених ресурсів, наприклад через вірус, на інших розділах може з'явитися помилка DoS.

Загроза від швидкого створення та переміщень ВМ. Сьогодні схему безпеки, коли мала кількість ВМ, адміністратори зберігають у контрольних таблицях. Якщо такий підхід поширений в організації з багатьма ВМ, то буде складно підтримувати безпеку віртуалізації в зв'язку зі швидкістю створення та переміщень ВМ.

Загроза від програмного забезпечення. Віртуалізація заснована на спеціальному програмному забезпеченні і це забезпечує появу багатьох потенційних уразливостей програмному забезпеченню, які можуть бути використані зловмисниками.

Загроза від віртуальних дисків. Віртуальні диски зазвичай зберігаються на хості як незахищені файли і отримати до них доступ дуже просто — не потрібно нічого зламувати.

Загроза від навантаження з різними рівнями довіри. Робочі навантаження з різними рівнями довіри можуть бути поміщені на один і той самий сервер або vswitch, і безпека цих робочих навантажень буде такою ж високою, як безпека найменш захищеного навантаження. Якщо на сервері знаходиться чутлива інформація, це може бути небезпечно.

Таким чином, стає зрозумилим, що найбільша небезпека для віртуалізованих ІТ-інфраструктур приховується в тому, що слабкі місця в рішеннях для віртуалізації дозволяють використовувати гостьову систему для виконання шкідливого коду через гіпервізор. Якщо зловмисник отримає повний контроль над гіпервізором, йому стануть доступні всі під'єднані розділи мережі, масові системи зберігання та віртуальні машини. Якщо раніше постраждати могли тільки окремі сервери і додатки, то тепер в зону ризику потрапляє відразу безліч ВМ через їх концентрацію на одному апаратному пристрої. У зв'язку з цим для контролю віртуального мережного трафіку і суворого дотримання директив необхідно вжити додаткових заходів безпеки в першу чергу щодо платформи віртуалізації, на якої працюють ВМ.

Відомо, що забезпечення захисту будь-якої складної системи починається з організаційних заходів [3; 4]. Звідси забезпечення захисту віртуалізованої ІТ-інфраструктури також починається з організаційних заходів.

Впровадження організаційних заходів починається у віртуалізації ІТ-інфраструктури з усунення звичного розподілу обов'язків: адміністраторів віртуального середовища і мереж. Для цього створюється безпека платформ віртуалізації, яка починається зі встановлення зон відповідальності і поділу обов'язків (Separation of Duties). Розглянемо приклади усунення загроз для віртуалізованої ІТ-інфраструктури за допомогою організаційних заходів.

1. Загроза безконтрольної маніпуляції з віртуальними машинами. Однією з найбільш актуальних загроз для віртуальної ІТ-інфраструктури є наявність деяких «суперкористувачів», коли адміністратори віртуальної інфраструктури можуть виконувати маніпуляції з віртуальними машинами зі своїх робочих місць і робити це безконтрольно. Відомо, що віртуальну машину (на відміну від фізичної) можна скопіювати, видалити або спотворити, тому традиційні методи захисту (наприклад, обмеження фізичного доступу та інші) для захисту віртуальної інфраструктури неспроможні. У зв'язку з цим виникає актуальне і своєчасне завдання щодо визначення вимог до захисту технологій віртуалізації. Вирішення цього завдання можливе за допомогою інструментів контролю всіх дій з управління віртуальною інфраструктурою і доступу до даних віртуальних машин. Йдеться про створення такого засобу, що дозволяє розмежувати доступ адміністраторів до віртуальної інфраструктури і контролювати дії адміністраторів. Одним із способів створення такого інструменту є організаційний.

Організаційний спосіб захисту віртуальної інфраструктури передбачає створення ланки інформаційної безпеки віртуальної інфраструктури, тобто адміністратора інформаційної безпеки віртуальної інфраструктури. Тоді такий інструмент буде надавати можливість обмежувати маніпуляції з віртуальними машинами інших адміністраторів (підлеглої ланки). Фактично це означає, що будь-які зміни в конфігурації віртуальної інфраструктури і розташування віртуальних машин не набувають чинності без підтвердження адміністратора інформаційної безпеки віртуальної інфраструктури.

2. Загроза для консолідації віртуальних машин. Наступною актуальною загрозою для віртуальної ІТ-інфраструктури є наявність проблеми консолідації ВМ різних рівнів конфіденційності в межах одного і того самого хоста. Для консолідації апаратного забезпечення ІТ-інфраструктури

застосовуються дві ключові технології віртуалізації: абстрагування і розподіл апаратних ресурсів. Відомо, що гостьові ОС і користувачі ізольовані від фізичних систем за допомогою шару віртуалізації. Реально доступні ресурси абстрактно і однорідно розподіляються гіпервізором між усіма ВМ. До теперішнього часу з міркувань безпеки окремі системи не були залучені для віртуалізації, але сьогодні вони стають вузьким місцем для підвищення ефективності розвитку ІТ-інфраструктури, а саме: треба або їх віртуалізувати, або виключити з процесів, що не завжди можливо. Вирішення цієї проблеми також може бути досягнуто організаційним способом, тобто створення ланки інформаційної безпеки віртуальної інфраструктури, тобто адміністратора інформаційної безпеки віртуальної інфраструктури. Тоді такий адміністратор також може сегментувати віртуальну інфраструктуру і самостійно вирішувати, на якому хості будуть виконуватися ті чи інші ВМ і з яким рівнем захисту. Це дозволить зняти проблему консолідації віртуальних машин різних рівнів конфіденційності в межах одного і того самого хоста [5].

3. Загроза уразливості платформ віртуалізації. Актуальною загрозою для віртуальної ІТ-інфраструктури є проблема уразливості самих платформ віртуалізації. Сьогодні уразливості платформ віртуалізації виправляються їх виробниками, але не всі використовують останні версії платформ і тим більше не всі налаштовують свою інфраструктуру відповідно до рекомендацій виробника. Ці рекомендації надаються вендорами у вигляді окремого документа з інструкціями, які потрібно виконати на хостах. Але виконувати ці рекомендації вручну досить незручно. Тому виникає завдання пошуку інструменту, що дозволить автоматизувати цей процес і вибрати для інфраструктури найбільш безпечну конфігурацію, відстежувати її незмінність, заносити в журнал всі події безпеки в режимі реального часу, оповіщати адміністратора інформаційної безпеки про порушення, а також формувати звіти про стан інфраструктури [5].

Рекомендації послідовності дій щодо забезпечення захисту віртуалізованої ІТ-інфраструктури:

1. ***Попередня організаційна робота.*** Це означає, що виконується прив'язка до централізованих каталогів, що забезпечує технічну підтримку розподілу повноважень. Розподіл повноважень досягається за допомогою ролей, що базуються на розподілі користувачів по групах. При цьому завжди необхідно діяти за принципом, згідно з яким повноваження для виконання тієї чи іншої дії обмежуються лише необхідним мінімумом (Principle of Least Privilege).

2. ***Зміцнення гіпервізора.*** Коли визначено організаційні рамкові умови, можна приступати до технічного захисту інфраструктури (рис. 1).

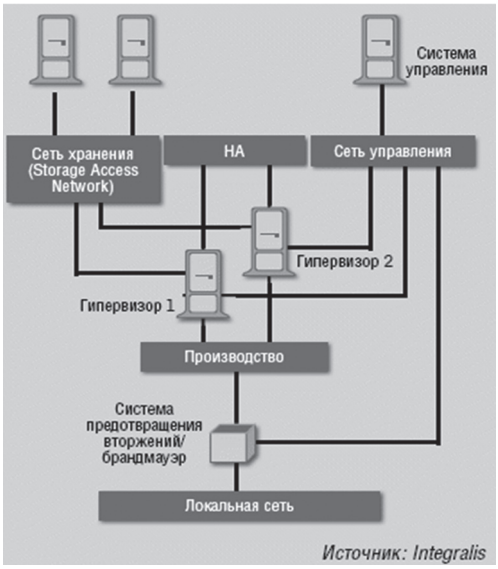

Рис. 1. Організаційні рамкові умови [5]

Оскільки гипервізор є базовою платформою для віртуалізації, він потребує особливого захисту. Усі виробники, що запроваджують рішення для віртуалізації публікують рекомендації щодо забезпечення безпеки, в яких описується, як потрібно зміцнювати відповідні системи після установки. Цим директивам слід приділити особливу увагу, оскільки за їх допомогою можна отримати надання тільки тих служб, які дійсно потрібні для віртуалізації.

3. ***Розробка мережної концепції.*** Ця можливість зниження потенційних ризиків полягає в розробці надійної мережної концепції. Центральні функції, такі як доступ до систем зберігання і засобів управління, повинні застосовуватися тільки в ізольованих сегментах мережі. Наприклад, є iSCSI (*Internet Small Computer System Interface*) — протокол, який базується на TCP/IP і розроблений для встановлення взаємодії і управління системами зберігання даних, серверами і клієнтами. Або VMotion — протокол, який визначає назву процесу динамічної міграції, тобто переїзду ВМ з одного сервера на інший без перерви в роботі. Ці протоколи використовуються без повного шифрування, і доступ до цих областей мережі повинен надаватися тільки авторизованим адміністраторам. Наступний приклад, фільтрацію зазвичай виконують брандмауери, які, особливо в поєднанні з системою запобігання вторгнень (IPS —Intrusion Prevention System), здатні забезпечити ефективний двосторонній захист віртуальної і фізичної інфраструктури. Ці приклади наочно вказують на наявність небезпек, прихованих в безпосередньому мережному оточенні віртуальної ІТ-інфраструктури. Крім небезпек, прихованих у безпосередньому мережевому оточенні віртуальної ІТ-інфраструктури, більшість атак здійснюється безпосередньо з ВМ. Таким чином, такі системи повинні захищатися

так само добре, як і фізичні. Для цього треба використовувати методи, які визначаються індивідуальними вимогами до безпеки віртуальних машин. Для цього спочатку слід провести класифікацію ризиків, а для розподілу віртуальних машин за групами використовувати критерії можливості безпеки завдання і комунікаційні відносини, що створює гостьова операційна система, яка виконується ВМ.

4. *Формування груп для додаткових заходів захисту*. Для сформованих груп можна забезпечити додаткові заходи захисту, добре знайомі адміністраторам за сферою безпеки фізичних серверів і клієнтів, наприклад, брандмауери і системи запобігання вторгнень, віртуальні приватні мережі VPN, шифрування і контроль мережного доступу (NAC — Network Access Control). Досі активація таких компонентів безпеки відрізнялася високою трудомісткістю у зв'язку з необхідністю здійснення додаткової сегментації, а для забезпечення можливості аналізу мережний трафік повинен був перенаправлятися через фізичні або віртуальні системи безпеки.

5. *Функції безпеки за допомогою програмного інтерфейсу програми API*. API (*Application programming interface*) — це програмний інтерфейс програми, інтерфейс прикладного програмування. У компанії VMware усвідомили цю проблему і впровадили в vSphere 4 інтерфейс безпеки під назвою VMsafe (рис. 2).

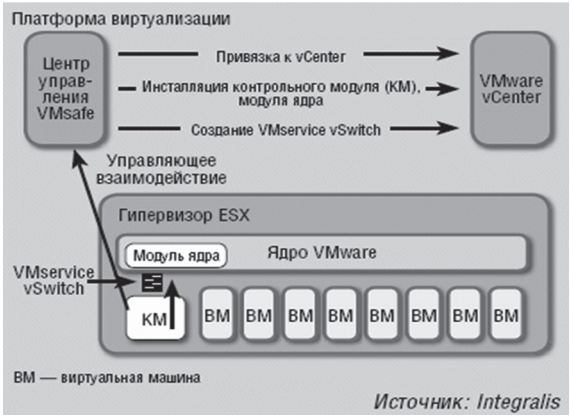

Рис. 2. Інтерфейс безпеки VMsafe [5]

Він дозволяє здійснювати прямий доступ до систем зберігання, процесорів, мереж, пакетних фільтрів, процесів і нагромаджувачів великого обсягу. Іменіті виробники вирішень безпеки використовують цей інтерфейс при розробці нового покоління продуктів, розрахованих на застосування в середовищі віртуалізації. Пряма інтеграція в ядро VMware дозволяє здійснювати фільтрацію даних без прив'язки до мережі, маршрутизації або програмним агентам, забезпечуючи максимальну продуктивність. Система безпеки VMsafe включає в себе кілька модулів: центр адміністрування для управління правилами, модуль ядра, що завантажується в ядро VMware, контрольний модуль у вигляді віртуальної машини. Контрольний модуль у вигляді віртуальної машини створює з'єднання з модулем ядра за допомогою спеціалізованого комутатора VMservice Vswitch, що дозволяє створювати з'єднання по TCP/IP. Через контрольний модуль система адміністрування управляє функціями безпеки в модулі ядра. Якщо контроль і подальше перенаправлення даних здійснюються в ядрі, то йдеться про реалізацію за технологією Fast Path, коли теоретично можна використовувати повну потужність гіпервізора. А якщо дані перенаправляються на віртуальний контрольний модуль, де здійснюється їх подальша перевірка, значить, застосовується метод Slow Path, що забезпечує помітно меншу продуктивність.

В основу цих інструментів захисту віртулізованих IT-інфраструктур покладено алгоритм дій для безпечної віртуалізації [5]: розробку надійної мережної концепції; організаційний розподіл ролей; установку і зміцнення системи управління; прив'язку до служби каталогів; установку гіпервізора; активацію захисних заходів для гіпервізора; установку/міграцію віртуальних машин; активацію захисних заходів для віртуальних систем; регулярну активацію і тестування резервних копій; контроль роботи за допомогою інструментів моніторингу.

Висновки

Орієнтація на безпеку у віртуальних середовищах IT забезпечує дотримання правил безпеки та виконання вимог, що висуваються до захисту мереж і даних, навіть в епоху віртуалізації і хмарних обчислень. Багато компаній, наприклад VMware, сприяють просуванню інновацій в області віртуалізації, однак зовсім скоро за нею підуть інші постачальники платформ віртуалізації. Уже зараз виробники рішень безпеки не обмежуються тільки продуктами VMware, плануючи надалі здійснювати інтеграцію на інші платформи.

Список використаної літератури

*1. **Технологии** виртуализации и защищенность информационных систем [Електронний ресурс]. URL:*

http://lib.itsec.ru/articles2/Oborandteh/tehnologii-virtualizacii-i-zaschischennostj-informacionnyh-sistem / (Дата перегляду 30 грудень 2019)

*2. **Рынок** виртуализации: новые возможности и новые риски [Електронний ресурс]. URL:*

https://www.itweek.ru/security/article/ detail.php?ID=164047/(Дата перегляду 30 грудень 2019)

*3. **Даник Ю. Г., Катков Ю. І., Пічугін М. Ф.** Національна безпека: запобігання критичним ситуаціям: монографія. Житомир: Рута, 2006. 386 с.*

*4. **Вишнівський В. В., Катков Ю. І., Сєрих С. О.** Роль і місце інформаційної інфраструктури під час виникнення явища критичності організаційної системи // Зв'язок. 2017. №5. С. 51–56.*

*5. **Виртуальные** серверы — реальные риски [Електронний ресурс]. URL: https://www.osp.ru/lan/2010/09/13004325/ (Дата перегляду 30 грудень 2019)*

*6. **Безопасность** виртуализации. Ч. 1 [Електронний ресурс]. URL: https://habr.com/ru/post/243845/ (Дата перегляду 30 грудень 2019)*

Ю. И. Катков, Ю. В. Березовская, Н. Н. Рыжаков, Д. С. Гнидюк

АНАЛИЗ РИСКОВ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИЯ И КОНТЕЙНЕРИЗАЦИИ В ОБЛАЧНЫХ СЕРВИСАХ

В статье рассматривается проблема последствий применения технологий виртуализации и контейнеризации в облачных сервисах. Применение виртуализированной ИТ-инфраструктуры приносит бизнесу массу преимуществ, а именно: позволяет сократить расходы, упростить эксплуатацию серверов и клиентских устройств. Однако одновременно возникают новые угрозы для безопасности данных и сетей, происходит увеличение информационных рисков и создаются условия для компрометация виртуальных машин. Поэтому решение по обеспечению защиты виртуализированной ИТ-инфраструктуры перестали быть исключительно техническими, теперь в них включаются организационные мероприятия и предусматриваются практические меры по устранению проблемных ситуаций. Причина увеличения информационных рисков заложена в самой природе виртуализации. Причина в том, что виртуальная инфраструктура отличается от физической двумя элементами: гипервизором и средством управления гипервизором. Гипервизор и средство управления им являются критическими элементами в виртуальной ИТ-инфраструктуре. Они создают угрозы для виртуализации ИТ-инфраструктуры. Описаны особенности этих угроз при внедрении виртуализации и контейнеризации в облачных сервисах. Показано, что наибольшая опасность для виртуализированной ИТ-инфраструктуры таится в том, что слабые места в решениях для виртуализации позволяют злоумышленнику влиять с помощью вредоносного кода на гипервизор хостовой операционной системы, поэтому создаются условия влиять на гостевые системы. Если злоумышленник получит полный контроль над гипервизором, ему станут доступны все подключенные разделы сети, массовые системы хранения и все виртуальные машины. Рассматриваются наиболее вероятные угрозы для виртуализированной ИТ-инфраструктуры, а именно: угроза бесконтрольной манипуляции с виртуальными машинами; угроза для консолидации виртуальных машин; угроза уязвимости платформ виртуализации. Предложены организационные меры обеспечения защиты виртуализированной ИТ-инфраструктуры путем укрепления гипервизора и разработки сетевой концепции. Рассмотрены инструменты защиты виртуализованнной ИТ-инфраструктуры.

Ключевые слова: виртуализация; контейнеризация; угроза; уязвимость; ИТ-инфраструктура.

Yu. I. Katkov, Yu. V. Berezovska, N. N. Ryzhakov, D. S. Gnidyuk

RISK ANALYSIS OF THE USE OF VIRTUALIZATION AND CONTAINERIZATION TECHNOLOGIES IN CLOUD SERVICES

The article considers the problem of the consequences of the use of virtualization and containerization technologies in cloud services. The use of virtualized IT infrastructure brings a lot of advantages to the business, namely: it allows to reduce costs, simplify the operation of servers and client devices. However, at the same time, new threats to the security of data and networks arise, information risks increase and conditions are created for the compromise of virtual machines. Therefore, the decision to ensure the protection of virtualized IT infrastructures has ceased to be exclusively technical, now they include organizational measures and provide practical measures to eliminate problem situations. The reason for the increase in information risks lies in the very nature of virtualization. The reason is that the virtual infrastructure differs from the physical in two elements: the hypervisor and the hypervisor management tool. The hypervisor and its management tool are critical elements in a virtual IT infrastructure. They pose a threat to the virtualization of IT infrastructure. The features of these threats during the implementation of virtualization and containerization in cloud services are described. It has been shown that the greatest danger to virtualized IT infrastructures lies in the fact that weaknesses in virtualization solutions allow an attacker to use the malicious code to influence the hypervisor of the host operating system; therefore, conditions are created to affect guest systems. If an attacker gains full control over the hypervisor, all connected sections of the network, mass storage systems, and all virtual machines will become available to him. The most probable threats to virtualized IT infrastructures are considered, namely: the threat of uncontrolled manipulation of virtual machines; threat to the consolidation of virtual machines; virtualization platform vulnerability threat. Organizational measures are proposed to ensure the protection of virtualized IT infrastructures by strengthening the hypervisor and developing a network concept. The tools for protecting virtualized IT infrastructures are considered.

Keywords: virtualization; containerization; threat; vulnerability; IT infrastructure.