HPE Zerto Cyber Resilience Vault

еталонний кіберзахист ваших даних

Hewlett Packard Enterprise operated by Sophela

Рішення проти кіберздирництва: програмно-апаратний комплекс від HPE забезпечує відновлення даних за будь-якого сценарію.

Рівень загроз і кібератак, пов'язаних зі здирництвом (ransomware), продовжує зростати, і вони стають дедалі серйознішими і витонченішими. Нещодавнє чергове дослідження IDC показало, що більшість інцидентів за останні 12 місяців було здійснено за допомогою шкідливого ПЗ для подальшого «викупу» зашифрованих даних. Вартість хакерської атаки продовжує знижуватися завдяки появі послуг з надання «викупу», а успішні зараження стимулюють розробку шкідливих програм нового покоління. Щоб мінімізувати ризики від різноманітних атак, IT-підрозділам необхідна потужна стратегія проактивного глибокого захисту для запобігання та припинення атак – так звана «Left of Boom»*. Не менш важливою є і стратегія «Right of Boom», спрямована на відновлення після атаки. Для швидкого виявлення, реагування та відновлення після атак ransomware організації повинні приділяти пріоритетну увагу обом стратегіям. Попри те, що превентивні рішення «Left of Boom» зараз ефективні як ніколи, до корпоративних IT ставлять дедалі жорсткіші вимоги.

Компанії, що займаються кіберстрахуванням (на жаль, поки що не в нашій країні), вимагають від підприємств посилення безпеки, зокрема створення спеціалізованих сховищ даних. У ЄС Закон про стійкість цифрових операцій, або скорочено DORA, перемикає увагу на безпеку і безперервність бізнесу. У США Комісія з цінних паперів і бірж (SEC) ввела суворі вимоги для публічних корпорацій, включно з визначенням сторін, відповідальних за стратегію кіберстійкості.

Традиційні системи зберігання наражають вас на ризик

Поширені методи забезпечення кіберстійкості ґрунтуються на ризикованих технологіях і архітектурах всіляких сховищ. Головним їхнім недоліком є швидкість або час відновлення. Витягнення старих резервних копій і відновлення з подібних нешвидких сховищ може розтягнути цей процес на дні або тижні. Сканування «чистих копій», що знаходяться в «чистих кімнатах», ще більше продовжує ці дії, як і відновлення на непродуктивних сховищах. Якщо спеціалізовані органи або служби безпеки проводять криміналістичний аналіз виробничої інфраструктури, вам може знадобитися на деякий час після відновлення запустити робочі навантаження в іншому місці, чого не можуть повноцінно забезпечити ні пристрої резервного копіювання, ні холодні хмарні сховища. Також вкрай важливо дуже швидко відновити бізнес-операції компанії, а для цього застарілі рішення для резервного копіювання та архівування поки що не підходять.

Існує кілька пропозицій, які здатні впоратися з перерахованими вище проблемами. Одна з яких — HPE Zerto. Це рішення від початку розроблялося для аварійного відновлення віртуальних середовищ, спершу з VMware vSphere, а потім також з Microsoft Hyper-V, але цього року чекаємо підтримки абсолютно нового рішення — HPE VM Essentials. HPE Zerto — це найкраще у своєму класі рішення для безперервного захисту даних з майже синхронною реплікацією. Ця технологія охоплює не тільки реплікацію в реальному часі кожної зміни даних, але також містить вбудоване виявлення та оповіщення про шифрування у реальному часі. Також існує і додаткове розширення до цього рішення — ***HPE Zerto Cyber Resilience Vault***. Воно засноване на трьох основних принципах: «реплікувати та виявляти», «ізолювати та блокувати», «тестувати та відновлювати» (**рис. 1**), все це побудоване на архітектурі нульової довіри. Додаткове розширення також має на меті допомогти компаніям підтримувати відповідність регуляторним вимогам у міру збільшення кількості державних постанов, зводячи до мінімуму ризик великих штрафів.

* Термін «Right of Boom» належить до дій і заходів у відповідь, що вживаються після того, як стався інцидент або атака у сфері кібербезпеки. Він відрізняється від терміна «Left of Boom», який охоплює заходи, вжиті до атаки, щоб запобігти їй або мінімізувати наслідки. Термін «Boom» означає момент зламу або успіху атаки. Усунення наслідків як «Left of Boom», так і «Right of Boom» має вирішальне значення для ефективної безпеки, оскільки дає змогу мінімізувати як імовірність, так і наслідки успішних атак.

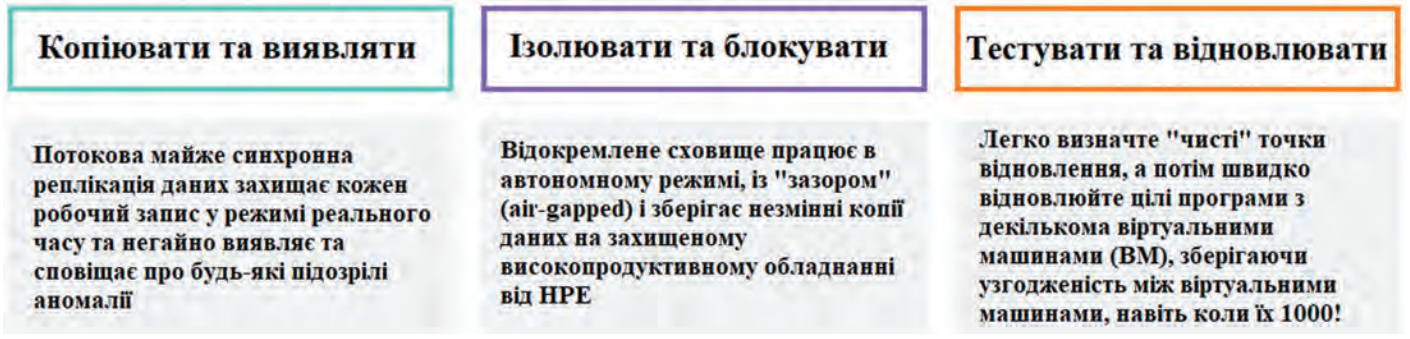

Рис. 1. Три принципи HPE Zerto Cyber Resilience Vault

Швидке відновлення за допомогою HPE Zerto

Рішення Zerto від компанії HPE надає підприємствам універсальне спеціальне сховище для кібервідновлення, призначене для захисту навіть від найбільш руйнівних сценаріїв зараження/шифрування шкідливим ПЗ. Сховище HPE Zerto Cyber Resilience Vault складається з трьох основних компонентів, що використовують децентралізовану архітектуру Zero Trust «з зазором» (air-gapped) для забезпечення швидкого відновлення.

Рис. 2. Склад рішення HPE Zerto Cyber Resilience Vault

До складу рішення (**рис. 2**) входять системи зберігання даних HPE Alletra Storage, сервери HPE ProLiant, мережеві комутатори HPE Aruba, програмне забезпечення HPE Zerto, а також дві ключові зони інфраструктури, що включають всі вищевказані компоненти.

Ключова функція HPE Zerto Cyber Resilience Vault полягає в тестуванні та відновленні робочих навантажень в ізольованій «чистій кімнаті» — vault zone. У цій інфраструктурі адміністратори можуть безпечно планувати дії з відновлення робочих навантажень, сканування вразливостей, щоб гарантувати відсутність програм-здирників у робочому навантаженні до його відновлення у виробничому середовищі на головному сайті. Інші дії можуть включати криміналістичне дослідження даних для розуміння того, як вони могли бути змінені, відстеження джерела зараження і багато іншого, і все це без впливу на виробничі робочі навантаження або інфраструктуру (**рис. 3**).

Landing zone

Landing zone на базі віртуального середовища VMware vSphere може бути локальною або віддаленою, а також слугувати традиційною ціллю аварійного відновлення, якщо вона розташована за межами головного сайту. Landing zone служить ціллю реплікації для безперервного захисту даних (CDP) за допомогою HPE Zerto. Реплікація CDP в HPE Zerto здійснюється без агентів, тому всередині захищеної віртуальної машини, або скорочено ВМ, немає нічого, що можна було б відключити або перехопити за допомогою шкідливого ПЗ. Кожен запис на захищених ВМ стискається, шифрується і відправляється в vault zone, де зберігається в динамічному журналі CDP — потоковому журналі тисяч точок відновлення. Журнал має задану користувачем історію тривалістю від однієї години до 30 днів і є першим найкращим найшвидшим варіантом для відновлення після виявлення шифрування.

Журнали та всі пов'язані з ними репліки закріплені за віртуальними застосунками,

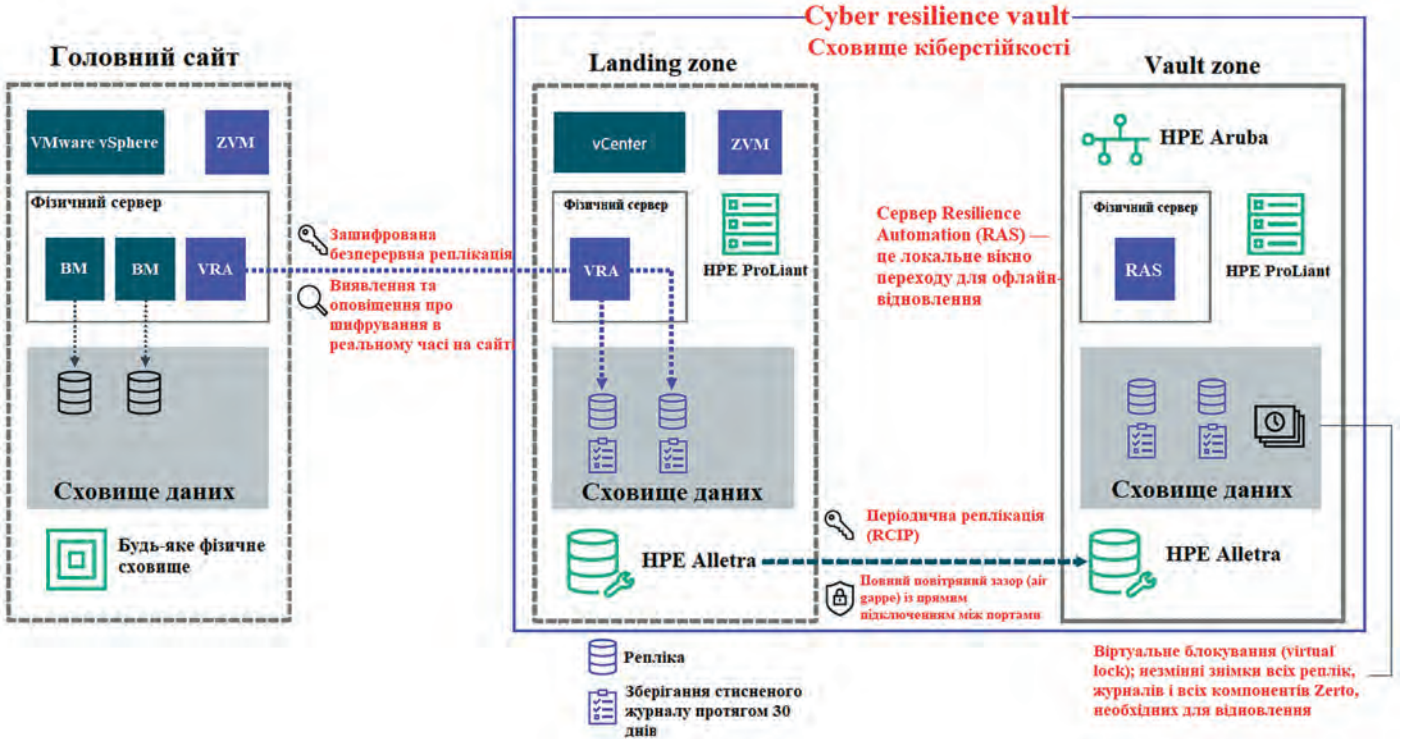

Рис. 3. Дві головні зони HPE Zerto Cyber Resilience Vault

що працюють на HPE ProLiant, а їхні сховища даних прив'язані до томів на СЗД HPE Alletra. Оскільки записи відображаються в журналі, вони також перевіряються за допомогою виявлення шифрування в реальному часі від HPE Zerto для раннього попередження про можливі зараження. Аналіз шифрування також доступний через API для подальшої оцінки та візуалізації за допомогою наявного стека рішень безпеки, якщо такий вже є на підприємстві.

Vault zone

Інша зона може бути фізично розташована разом/поряд з landing zone, і в ній також знаходиться обладнання HPE ProLiant і HPE Alletra. Але ця ізольована зона зберігання, або «чиста кімната», повністю «герметична» і не має доступу до Інтернету або виробничої мережі. Оскільки централізована площина управління відсутня, у сховищі немає відкритого порту управління і немає єдиної точки компрометації. HPE Alletra в landing zone і HPE Alletra в vault zone використовують пряме під'єднання для віддаленого копіювання через IP (RCIP) для реплікації всіх даних з однієї зони в іншу, включно з журналами та репліками HPE Zerto, у режимі «точка-точка». Цей підхід поєднує в собі найкращі якості синхронної реплікації — наприклад, наднизькі значення цільової точки відновлення (RPO) і високу продуктивність, — і традиційних асинхронних підходів: наприклад, вищу стійкість до високих затримок каналів. Нарешті, Resilience Automation Server (RAS) у vault zone — це невеликий сервер, який запускає критично важливі служби та працює з власними службами HPE Aruba і HPE Alletra для управління ключовими заходами кіберстійкості.

Процес відновлення

Архітектура HPE Zerto охоплює різні по своїй складності сценарії відновлення після зараження, зокрема такі.

Зараження файлів/папок/ВМ: якщо радіус ураження здирницьким ПЗ обмежений файлами та папками на ВМ, їх можна практично миттєво відновити з вихідного місця розташування за тимчасовою міткою журналу HPE Zerto, яка знаходиться всього за 5–15 секунд до зараження. Якщо одна або кілька ВМ зашифровані за допомогою програми-здирника, HPE Zerto може практично миттєво відновити їхню працездатність без будь-яких проміжних кроків — наприклад, переміщення сховища vMotion.

Повне зараження робочого навантаження: якщо були заражені всі ВМ на виробничому/головному сайті, але в landing zone вони все ще не заражені, то повне відновлення працездатності може бути здійснене за лічені хвилини. Оскільки HPE Alletra — це повністю all-flash рішення, призначене для критично важливих робочих навантажень, застосунки можна запускати з цього вторинного сайту без зниження продуктивності і без необхідності міграції на додаткове резервне сховище, здатне виконувати корпоративні інтенсивні робочі навантаження.

Зараження декількох сайтів: якщо основний сайт і landing zone не працюють — наприклад, зашифровані всі дані на серверах навіть попри сегментацію мережі, — то vault zone з усього рішення HPE Zerto Cyber Resilience Vault стає найбезпечнішою «чистою кімнатою» для відновлення. У загальних рисах процес відновлення буде виглядати наступним чином:
– треба перебудувати сайт відновлення: всередині ізольованого сховища в vault zone використовуватиметься незмінний знімок для повторного розгортання VMFS зі збереженням UUID-підписів віртуальної інфраструктури;
– завдяки кіберстійкості HPE Zerto віртуальні менеджери та механізми переміщення даних у віртуальному середовищі будуть підключатися до мережі та відновлювати роботу без будь-якого ручного переконфігурування або налаштування;
– за допомогою журналу HPE Zerto вибирають одну з тисяч доступних точок відновлення, щоб відновити всі ВМ у вибраному порядку завантаження. Завдяки механізму оркестрування HPE Zerto в поєднанні з високою продуктивністю HPE Alletra цільовий час відновлення (RTO) вимірюється хвилинами або годинами, а не днями або тижнями. Стеки застосунків для декількох ВМ швидко підключаються до мережі точно в один і той самий момент часу, що зводить до мінімуму ручне керування.

Висновки

Завдяки HPE Zerto Cyber Resilience Vault у компаній з'явилося безпечне і високопродуктивне рішення для боротьби з різноманітними загрозами здирництва. Унікальна децентралізована архітектура HPE Zerto забезпечує швидке відновлення зі сховища «з зазором» (air-gapped) навіть після найсерйознішої кібератаки. Завдяки цьому з'являється:
- значне скорочення часу простою після атаки та уникнення прямої або непрямої втрати доходів;
- допомога в забезпеченні відповідності вимогам, таким як HIPAA, DORA, GDPR, SOX або FISMA/NIST SP 800–34;
- зниження складності завдяки наданню одним постачальником єдиного рішення, що складається з найкращого у своєму класі ПЗ та обладнання на кожному етапі ланцюжка кібервідновлення.

І останнє. Подібні кіберсховища слугують ключовим засобом забезпечення відповідності, надаючи безпечне середовище для зберігання конфіденційних даних та управління ними, полегшуючи аудит і забезпечуючи дотримання нормативних вимог.

Михайло ФЕДОСЄЄВ,
архітектор інфраструктурних рішень
Lantec
+38 044 360–56–27,
office@lantec.ua, https://lantec.ua