Ізоляція резервних копій у стратегіях захисту даних

Щоб убезпечити дані від сучасних кіберзагроз, варто використовувати додатковий рівень захисту: середовище автономних копій.

Хакерські атаки на IT-інфраструктуру приватних та державних організацій стали невід'ємною частиною сучасного світу. Останні кілька років взагалі виявилися рекордними для кіберзлочинців, які досягли найвищих показників фінансових збитків, що їх вони спричинили глобальній економіці за допомогою різноманітного шкідливого ПЗ. А головне — все вказує на те, що далі ситуація з кіберзагрозами буде лише погіршуватись.

Чи можуть IT-фахівці та фахівці з безпеки вжити заходів, які дозволять підготуватися до неминучої атаки та її наслідків? На щастя, завдяки резервному копіюванню бізнес має можливість надійно захистити свої критично важливі дані від катастроф, збоїв та атак кіберзлочинців — навіть у випадку обходу останніми кіберзахисту. Превентивне запобігання атаці є найкращим захистом, і провідні світові стандарти з кібербезпеки обґрунтовано наголошують на важливості правильної стратегії резервного копіювання. Розгляньмо їх детальніше.

Стратегія «3–2–1»

Найпопулярнішою є стратегія резервного копіювання «3–2–1», або — «золоте правило» захисту даних. Це доступне і просте рішення, яке потребує трьох (3) копій даних та використовує як мінімум два (2) типи носіїв; причому одна (1) копія знаходиться за межами організації. Зазвичай продуктивні дані — це копія №1; дані резервної копії в локальному репозиторії — копія №2; а копія №3 — дані за межами офісу для аварійного відновлення («стрічка», диск або хмарне сховище).

Але чи захищена ця стратегія від, наприклад, програм-вимагачів? Ні, бо жодна зі стратегій не забезпечує 100% захисту. Існує безліч способів оминути стратегію «3–2–1». Крім того, сьогодні атаки кіберзлочинців націлені вже на самі системи резервного копіювання, які можуть бути втрачені разом з рештою даних. Враховуючи нові виклики, рекомендується використовувати додатковий захист від програм-вимагачів: незмінність (immutability) та/або ізоляція резервних копій.

Стратегія «3–2–1–1–0»

Ізоляція даних не є чимось новим, і багато організацій вже додали її до класичної стратегії «3–2–1». Традиційно дані ізолювалися на магнітних стрічках, і цей підхід забезпечує чудовий рівень безпеки. Але відновлення часто займає багато часу, що є неприйнятним у вимогах безперервності бізнесу. Тому для якісного та гнучкого захисту організації звертаються до більш надійної та сучасної стратегії «3–2–1–1–0» (**рис. 1**). Вона розширює стратегію «3–2–1» — додані до правила номери «1–0» передбачають, що:

- 1 (одна) додаткова резервна копія має бути «автономною» — незмінною/недоступною до змін, через так звану операційну ізоляцію (air-gapping);
- 0 — відсутність помилок (ця копія не повинна мати помилок). Тобто наявність перевірки цілісності резервних копій даних.

Ці додаткові опції допомагають забезпечити найвищий рівень можливості відновлення даних після будь-якої катастрофи.

Ізоляція резервних копій

Ізольована резервна копія захищає від дій кіберзлочинців та гарантує, що критичні резервні копії залишаться відключеними та неушкодженими, навіть якщо продуктивне середовище буде скомпрометоване. Існує два основних типи ізоляції резервних копій.

1) **Фізична ізоляція** — відключення сховища від продуктивної мережі. Це реальна ізоляція даних на фізичному рівні, яка часто пов'язана із зовнішніми носіями: резервними копіями на стрічці, які підключаються/відключаються вручну.

2) **Логічна ізоляція** — коли цільове сховище фізично підключене, але ізольоване від мережі логічно. Це означає, що носій даних фізично перебуває у підключеному стані, але доступ до даних має певні обмеження.

Логічна ізоляція вимагає менше часу для налаштування і не зазнає впливу людських помилок, а також дозволяє автоматизувати процес, забезпечити більш високу частоту створення резервних копій та відновлювати дані практично миттєво. При логічній ізоляції для зберігання резервних копій використовуються не окремі пристрої, а так звані ізольовані томи/розділи зберігання. Для створення невидимого бар'єру між даними та самим доступом до даних логічна ізоляція покладається на технології безпеки: доступ на рівні ролей, шифрування, використання програмно-конфігурованої мережі.

Томи/розділи зберігання підключаються до основного репозиторію копій тільки для збереження критично важливих даних, а далі відключаються. Підключення та відключення ізольованих томів може здійснюватися вручну або автоматично. Вбудоване ПЗ автоматизує синхронізацію даних між продуктивними системами та сховищем та може створювати незмінні резервні копії з заблокованими політиками зберігання. У разі збою ізольовані томи можна увімкнути, а дані, що зберігаються на них, — відновити.

Оскільки томи за замовченням «відключені» і недоступні для застосунків, користувачів та виробничих навантажень, вони захищають резервні копії, що зберігаються, від збоїв на основному продуктивному середовищі.

Рис. 1. Стратегія ізолювання резервних копій

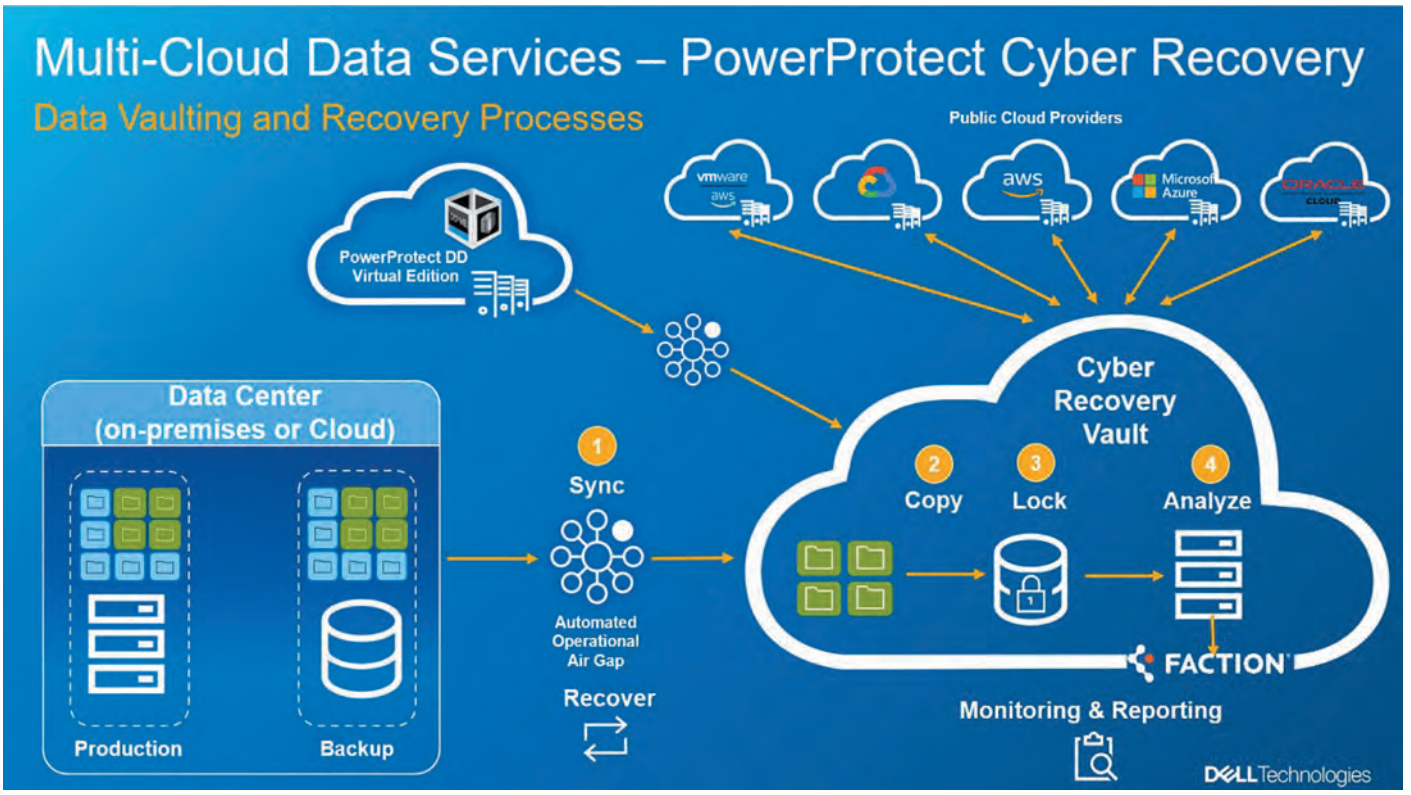

Рис. 2. Платформа Dell PowerProtect Cyber Recovery

Сховища даних Dell PowerProtect Cyber Recovery

Сьогодні на ринку з'являється дедалі більше спеціалізованих продуктів, які поєднують кілька рівнів захисту та безпеки в одне готове рішення. Це спеціально розроблені пристрої резервного копіювання з функціями операційної ізоляції, з вбудованими мережевими компонентами та контролерами живлення, які автоматично ізолюють та відключають пристрій від продуктивного середовища.

Такі рішення орієнтовані на великі підприємства та зазвичай є компонентами більш складних та комплексних систем кіберзахисту: наприклад, Dell PowerProtect Cyber Recovery (**рис. 2**).

Dell PowerProtect Cyber Recovery – це рішення для управління даними, їх захисту та відновлення, що використовує кілька резервних копій — після створення вони копіюються в ізольоване сховище для захисту та аналізу.

Платформа містить одне або кілька сховищ (vaults), які можуть розташовуватись локально на пристрої PowerProtect DD або в хмарі, за допомогою програмного рішення Dell APEX Protection Storage for Public Cloud. В обох випадках сховище є ізольованим, тобто відокремленим від робочого — фізично у разі локального розгортання або логічно у середовищі APEX.

Налаштування та впровадження таких систем вимагає додаткових знань, досвіду та аналізу інфраструктури — тому такі роботи краще довірити компаніям, що мають відповідну кваліфікацію: наприклад, SNT Ukraine, яка є Dell Technologies Platinum Partner.

Рішення для резервного копіювання від Veeam

СМБ краще звернути увагу на більш доступні рішення, модернізувати компоненти існуючої системи або додати елементи ізоляції резервних копій. Можливі заходи:

1) виведення сервера резервного копіювання з доменної інфраструктури — подальше підключення будь-якого NAS-пристрою на окремий мережевий порт цього сервера, що не має доступу до корпоративної мережі, створить певну ізоляцію цих даних від решти мережі;

2) підключення додаткового захищеного репозиторію резервних копій для незмінності даних. Його можна розгорнути на фізичному сервері під управлінням ОС Linux та відповідного ПЗ системи PKiB (наприклад, Veeam Hardened Repository);

3) зменшення вікна можливостей для атаки. Впровадити програмні сценарії, що вимикають мережеві порти для пристроїв репозиторію і вмикають лише на час виконання задач з резервного копіювання;

4) використання хмарних сховищ для автономних репозиторіїв резервних копій. AWS і Azure мають можливості налаштування політик, які не дозволяють файлам змінюватись протягом певного часу, після чого вони автоматично видаляються або продовжують зберігатися.

Комбінація таких заходів дозволяє наблизитись до ізольованості та незмінності резервних копій. Цього можна досягти, наприклад, використавши платформу Veeam Data Platform — комплексне рішення для швидкого, надійного та безпечного резервного копіювання й відновлення.

Veeam пропонує надійне і практичне забезпечення незмінності резервних копій. Ізоляція у Veeam працює з кількома технологіями зберігання: об'єктне сховище (Object Storage), сховище типу Write-Once-Read-Many (WORM), Veeam Vault (хмарне спеціалізоване рішення від Veeam).

Основними перевагами стратегії «3–2–1–1–0» є захист від програм-вимагачів та інших шкідливих програм, оскільки резервні копії недоступні з сервера резервного копіювання або іншого місця в мережі. Ці дані залишаються в автономному режимі та захищені від атак завдяки ізольованому сховищу, забезпечуючи ще й довгострокове їх збереження.

Євген СЕРЕДОВИЧ, *старший інженер,*
компанія **SNT Ukraine**
+380 (44) 238–63–88
info@snt.ua, www.snt.ua