https://orcid.org/0000-0002-5080-1856
https://orcid.org/0009-0000-9667-1770

УДК 004.056.5

Ю.М. ЛИСЕЦЬКИЙ[*], Є.П. СЕРЕДОВИЧ[*]

ВИБІР ЕФЕКТИВНОЇ СТРАТЕГІЇ РЕЗЕРВНОГО КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна

Анотація. *Останні кілька років стали рекордними для кіберзлочинців, які завдали шкоди організаціям за допомогою різноманітних шкідливих програм. Превентивне запобігання атаці є найкращим захистом, а багато рекомендацій наголошують на важливості наявності для організації правильної стратегії резервного копіювання даних. Однак з урахуванням зростання складності та різноманітності IT-систем і кіберзагроз, сьогодні непросто вибрати ефективну стратегію резервного копіювання даних, яка б захищала всі критично важливі дані організації і зводила до мінімуму втрату даних та час простою. Тому у статті розглядається питання вибору ефективної стратегії резервного копіювання та відновлення даних. Як така стратегія пропонується стратегія «3-2-1-1-0», в основі якої знаходиться концепція «повітряного зазору» або «повітряної ізоляції», що передбачає наявність бар'єру, зведеного між самими даними резервного копіювання та доступом до цих даних. Це додаткова функція захисту даних, що використовується для ізоляції та відключення цільових пристроїв зберігання від незахищених мереж, виробничих середовищ і хост-платформ. Основними перевагами використання цієї стратегії є захист від програм-вимагачів та інших шкідливих програм, оскільки резервні копії недоступні з сервера резервного копіювання або іншого місця в мережі. Резервні дані залишаються в автономному режимі та захищені від таких атак завдяки ізольованому сховищу, забезпечуючи у такий спосіб ще й довгострокове збереження даних. Незмінність резервних копій є найважливішою складовою надійної стратегії захисту даних. Об'єднавши її з ізольованим сховищем, організації можуть підвищити безпеку та цілісність своїх резервних копій, гарантуючи, що дані залишаються у безпеці від онлайн-загроз, забезпечуючи високий рівень захисту. Оскільки цифрове середовище продовжує розвиватися, потреба в незмінних резервних копіях із ізольованим сховищем стає все більш очевидною як для організацій, так і для державних установ та відомств.*

Ключові слова: *кіберзлочинці, атака, захист даних, стратегія, резервне копіювання, концепція, повітряний зазор.*

Abstract. *The last few years have been record-breaking for cybercriminals, who have caused harm to organizations through various malicious programs. Preventative measures are the best protection, and many recommendations emphasize the importance of having a proper data backup strategy in place for organizations. However, considering the increasing complexity and diversity of IT systems and cyber threats, choosing an effective data backup strategy that would protect all critical organizational data while minimizing data loss and downtime is no easy task today. The article addresses the issue of selecting an effective data backup and recovery strategy. The recommended strategy is the 3-2-1-1-0 rule based on the concept of an «air gap» or «air isolation», implying the creation of a barrier between the backup data and access to that data. This additional data protection feature is used to isolate and disconnect target storage devices from unprotected networks, production environments, and host platforms. The main advantages of using this strategy are the protection against ransomware and other malicious software, since backup copies are inaccessible from the backup server or another network location. Backup data remains offline and protected from such attacks due to isolated storage, ensuring long-term data preservation as well. The immutability of backup copies is the most important component of a reliable data protection strategy. When combined with isolated storage, organizations can increase the security and integrity of their backup copies, ensuring that the data remains safe from online threats, providing a high level of protection. As the digital environment continues to evolve, the need for immutable backup copies with isolated storage is becoming more apparent to both organizations and government institutions.*

Keywords: *cybercriminals, attack, data protection, strategy, backup, concept, air gap.*

DOI: 10.34121/1028-9763-2025-1-76-80

1. Вступ

Останні кілька років стали рекордними для кіберзлочинців, які завдали шкоди організаціям за допомогою різноманітних шкідливих програм. Цілком зрозуміло, що дані є ключовим активом для будь-якої організації і що цей актив може бути важко захистити. Завдяки резервному копіюванню даних можна захищати свої критично важливі дані від можливих катастроф, збоїв системи та атак програм-вимагачів, щоб була можливість продовжувати свою повсякденну роботу без будь-яких перерв [1]. Превентивне запобігання атаці є найкращим захистом, а багато рекомендацій наголошують на важливості наявності для організації правильної стратегії резервного копіювання даних, тому що вона допоможе забезпечити ефективний захист даних та гарантувати надійну роботу організації. Однак з урахуванням зростання складності та різноманітності IT-систем і кіберзагроз сьогодні непросто вибрати ефективну стратегію резервного копіювання даних, яка б захищала всі критично важливі дані організації і зводила до мінімуму втрату даних та час простою, тому розв'язання цього питання є дуже актуальним.

Метою статті є визначення ефективної стратегії резервного копіювання та відновлення даних.

2. Стратегії резервного копіювання

Найпопулярнішою і, можливо, найстарішою є стратегія резервного копіювання «3-2-1». Стратегія резервного копіювання «3-2-1» — золоте правило захисту даних. Вона стала реальністю ще до бурхливого сплеску розвитку хмарних технологій [2]. Стратегія була орієнтована на використання доступних технологій (систем резервного копіювання, стрічкових масивів тощо) для створення максимально надійної системи захисту даних від більшості IT-ризиків, включаючи стихійні лиха, перебої в подачі електроенергії, віруси або шкідливі програми, а також пошкодження чи втрату даних.

Це недороге і просте рішення, яке потребує трьох (3) копій даних, використовуючи як мінімум два (2) типи носіїв, причому одна (1) копія знаходиться за межами центру обробки даних (ЦОД). Для більшості організацій продуктивні дані — це Копія № 1; дані резервної копії в локальному репозитарії — Копія № 2; а Копія № 3 — копія за межами майданчика для аварійного відновлення (зазвичай стрічка, диск або хмарне сховище).

Але чи захищена дана стратегія резервного копіювання від програм-вимагачів? Відповідь очевидна — жодна стратегія резервного копіювання не забезпечує 100 % захист від кіберзагроз. Існує безліч способів оминути стратегію «3-2-1». Крім того, сьогодні атаки програм-вимагачів націлені вже на самі системи резервного копіювання (СРК) [3]. Це робиться з метою унеможливити будь-які засоби та можливості аварійного відновлення. Резервні копії можуть бути зашифровані разом з рештою даних. Враховуючи ці нові виклики, експерти з безпеки рекомендують використовувати додатковий захист від програм-вимагачів, такий як незмінність (immutability) та/або ізоляція резервних копій, за допомогою так званого «повітряного зазору» (air-gapping).

Ізоляція даних не є чимось новим, і багато організацій вже зробили її частиною своєї класичної «3-2-1» стратегії резервного копіювання та відновлення. Традиційно дані ізолювалися на магнітних стрічках, а потім поверталися на місце у разі збою даних. Цей підхід забезпечує чудову безпеку, але відновлення часто займає багато часу, що призводить до недотримання угод про рівні обслуговування — SLA (Service Level Agreement), що просто неприйнятне у світлі сучасних вимог до безперервності функціонування організації. Щоб залишатися гнучкими та одночасно захищати дані, організації оновлюють свої правила резервного копіювання до більш надійної та сучасної стратегії «3-2-1-1-0».

Стратегія «3-2-1-1-0» розширює стратегію «3-2-1». Додані до правила номери 1-0 передбачають, що:

• одна додаткова резервна копія має бути «автономною», незмінною або недоступною до змін через так званий «повітряний зазор»;

• 0 — відсутність помилок (ця копія не повинна мати помилок), тобто, наявність перевірки цілісності резервних копій даних.

Ця стратегія допомагає забезпечити найвищий рівень можливості відновлення даних після будь-якого типу катастрофи.

Впровадження автономної ізольованої резервної копії (з так званим «повітряним зазором») є мірою захисту даних від атак програм-вимагачів і гарантує, що критичні резервні копії та репліки залишаться відключеними й неушкодженими, навіть якщо все продуктивне середовище та ЦОД будуть скомпрометовані. Перевірки цілісності даних допомагають знизити ризик людських помилок та пошкодження резервних копій.

3. Концепція «повітряного зазору»

Концепція «повітряного зазору» або «повітряної ізоляції» передбачає наявність бар'єру, зведеного між самими даними резервного копіювання та доступом до цих даних. Це додаткова функція захисту даних, що використовується для ізоляції та відключення цільових пристроїв зберігання від незахищених мереж, виробничих середовищ та хост-платформ.

Існують два основні способи ізоляції резервних копій:

• Фізична ізоляція — коли цільове сховище/репозиторій фізично ізольоване/відключене від продуктивної мережі. Цей тип являє собою реальну ізоляцію даних на фізичному рівні, які повністю відключені від мережі і знаходяться в автономному режимі. Його часто пов'язують із зовнішніми носіями інформації, наприклад, резервними копіями на стрічці, автономними стрічковими масивами/бібліотеками або додатковими системами зберігання, які підключаються або відключаються вручну. Тобто одержати дані з таких носіїв можна лише через фізичний контакт. Цей процес забирає багато часу і здатний привести до помилок. Звідси відсутність коротких показників часу відновлення (Recovery Time Objective — RTO) та гарантованих показників точки відновлення (Recovery Point Objective — RPO) — проміжків часу між збереженими резервними копіями.

• Логічна ізоляція — коли цільове сховище/репозиторій фізично підключене, але логічно ізольоване або відключене від мережі. Це означає, що носій даних фізично перебуває у підключеному стані, але доступ до даних має певні обмеження.

Варто відзначити, що у порівнянні з фізичною, логічна ізоляція резервного копіювання вимагає менше часу для налаштування та управління і не схильна до впливу людських помилок, що дозволяє автоматизувати робочий процес. Має більш високу частоту створення резервних копій та можливості практично миттєвого відновлення даних.

Враховуючи всі ці обставини, сучасні системи резервного копіювання та відновлення (СРКіВ) у більшості випадків починають відходити від використання повністю фізичної ізоляції резервних копій. Стратегія «3-2-1-1-0» передбачає використання переважно логічної моделі ізоляції як автономну копію даних або різноманітні комбінації цих двох типів.

З практичної точки зору, реалізація даної моделі ізоляції полягає в тому, що для зберігання резервних копій, знімків та реплік, СРКіВ використовують не реальні окремі пристрої, а так звані ізольовані томи/розділи зберігання. Важливо відзначити, що для створення невидимого бар'єру між даними та самим доступом до даних логічна ізоляція більше покладається на технології безпеки, такі як управління доступом на основі ролей, шифрування та хешування, використання програмно-конфігурованої мереж та ін.

Томи/розділи зберігання підключаються до основного репозиторію резервних копій тільки для збереження критично важливих даних, а потім відключаються. В залежності від програмного забезпечення (ПЗ) та виробника можливість підключення та відключення ізо-

льованих томів може здійснюватися вручну або автоматично, за допомогою налаштованих політик. Вбудоване ПЗ автоматизує синхронізацію даних між продуктивними системами та сховищем і може створювати незмінні резервні копії із заблокованими політиками зберігання. У разі збою на основному майданчику ізольовані томи можна увімкнути, а дані, що зберігаються на них, можна використовувати для операцій швидкого і безперешкодного відновлення.

Оскільки ізольовані томи, за замовчуванням, «відключені» і недоступні для додатків, баз даних, користувачів та робочих навантажень, які працюють у виробничому середовищі, вони захищають резервні копії, що зберігаються, від будь-яких збоїв, які можуть вплинути на основне продуктивне середовище.

4. Рекомендації щодо впровадження СРКіВ

На ринку все більше з'являється спеціалізованих продуктів, які поєднують кілька рівнів захисту та безпеки в одне готове рішення, що забезпечує максимальний захист критично важливих даних. Це спеціально розроблені пристрої резервного копіювання з функціями «повітряного зазору», з вбудованими мережевими компонентами та контролерами живлення, які автоматично ізолюють та відключають пристрій від продуктивного середовища відповідно до політик, визначених користувачем.

Такі рішення переважно орієнтовані на великі організації з великими об'ємами даних. Здебільшого ці рішення є компонентами більш складних та комплексних систем кіберзахисту та кібервідновлення, наприклад, Dell PowerProtect Cyber Recovery. Налаштування та впровадження таких систем вимагають додаткових знань, відповідного досвіду та детального аналізу інфраструктури, тому такі роботи краще довіряти компаніям-інтеграторам, які мають відповідну кваліфікацію.

Малим та середнім організаціям краще акцентувати увагу на більш доступних рішеннях. А саме: в рамках уже існуючих СРК трохи модернізувати деякі компоненти до рівня СРКіВ або додати окремі елементи незмінності/ізоляції даних резервних копій. Для цього можна запропонувати такі рекомендації:

• якщо сервер резервного копіювання виводиться з доменної інфраструктури організації — це вже додатковий рівень безпеки. А далі, якщо до цього сервера на окремий мережевий порт, що не має доступа до корпоративної мережі та Інтернету, підключити будь-який NAS-пристрій (як сховище для ізольованих резервних копій), то вже отримаєте деякий «повітряний зазор» у тому сенсі, що решта мережі не може отримати доступ до файлів, лише резервний сервер;

• також до основних локальних репозиторіїв резервних копій можна додати захищений репозиторій, який може забезпечити незмінність даних, що там зберігаються (тобто резервних копій). Його можна розгорнути на будь-якому фізичному сервері під управлінням ОС Linux та відповідних компонентів ПЗ, що вже можуть бути у складі існуючої СРКіВ (наприклад, Veeam Hardened Repository);

• створити частковий повітряний проміжок, запустивши в інфраструктуру тимчасові сценарії, що вимикають мережеві порти для пристроїв репозиторію або мережевих комутаторів і вмикають лише на час, коли заплановано повторення нових резервних копій. Це зменшує вікно можливостей для атаки;

• використовувати публічні та приватні хмарні сховища як автономні репозиторії резервних копій. Зокрема, Amazon і Microsoft Azure мають можливості налаштування політик, які не дозволяють жодному файлу змінюватись чи видалятися протягом певного часу, після чого вони автоматично видаляються політикою сегмента або продовжують зберігатись більш тривалий час за допомогою можливостей архівування.

І хоч такі окремі способи не можуть у повному обсязі забезпечити ізольованість та незмінність резервних копій, але, комбінуючи їх разом, можна максимально наблизитись до бажаних результатів.

5. Висновки

Основними перевагами використання стратегії резервного копіювання «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. Резервні дані залишаються в автономному режимі й захищені від таких атак завдяки ізольованому сховищу, забезпечуючи у такий спосіб ще й довгострокове збереження даних.

Незмінність резервних копій є найважливішим аспектом надійної стратегії захисту даних. Об’єднавши її із ізольованим сховищем, організації можуть підвищити безпеку та цілісність своїх резервних копій, гарантуючи, що дані залишаються у безпеці від онлайн-загроз, забезпечуючи високий рівень захисту. Оскільки цифрове середовище продовжує розвиватися, потреба в незмінних резервних копіях із ізольованим сховищем стає все більш очевидною як для організацій, так і для державних установ та відомств.

СПИСОК ДЖЕРЕЛ

1. Резервне копіювання — важливий крок до захисту від втрати. URL: https://production-ready.dev/2023/07/osoblyvosti-rezervnoho-kopiiuvannia/ (дата звернення: 02.03.2024).
2. Три стратегії резервного копіювання для захисту даних. URL: https://introserv.com/ua/blog/tri-strategii-rezervnogo-kopiyuvannya-dlya-zahistu-danih/ (дата звернення: 14.03.2024).
3. Лисецкий Ю.М. Защита информации: системы резервного копирования. *Системный анализ и информационные технологии. SAIT 2018:* сборник тезисов 20-ой междунар. научн.-практ. конф. (г. Киев, 21–24 мая 2018 г.). К.: УНК «ИПСА», НТУУ «КПИ, 2018. С. 236–237.

Стаття надійшла до редакції 17.05.2023