Предложения за промени в правилото 3-2-1, използвано в корпоративните стратегии за резервно копиране на данни в IT инфраструктурите

Михаил Радев

Proposals for changes in the rule 3-2-1 used in corporate backup strategies in the IT infrastructure

Mihail Radev

Abstract

The study focuses on the strategy to backup data, which any company has to develop and follow. An integral part of this strategy is the rule 3-2-1 for backup data. We suggest changes and additions to this rule in order to achieve a high degree of fault tolerance and reliability of the data. The rule and the changes suggested by us have to be complied strictly only if the value of data protection does not exceed the value of the data. In such cases, the same rule is followed but in partial fulfilment.

The combination of the rule of backup, recovery and mandatory pilot IT audits guarantee the health of companies' data.

*Keywords: b*ackup, 3-2-1 rule, corporate backup strategy, cloud backup service

„Ти си толкова добър системен администратор, колкото е добро последното ти резервно копие на данните“

Неизвестен автор

Често в IT средите се казва, че има два вида хора – такива, които са губили данни и такива, на които това им предстои. Целта на настоящата публикация е да намали броя на вторите.

Резервното копиране на данните във всяка компания би трябвало да е част от цялостна стратегия за резервно копиране и възстановяване. Тази стратегия би трябвало да започне с определяне на желания краен резултат и оттам да се изведат задачите и политиките за осъществяването му.[1] Крайният резултат е желаната възможност за възстановяване на системата. Възстановяване на данните се изисква по различни причини и те водят след себе си последващите решения, като създаване на политика и времеви график за създаване на резервни копия. Ефективното резервно копиране на данните включва и дефиниране на приоритети за данните, от които следва и избора на метода за създаване на резервни копия – например, жизнено важни данни, значително важни; важни; маловажни; нищожни. На база на дефинираните приоритети се определя вида резервно копиране, който е подходящ за конкретните данни: пълно резервно копиране – прави се резервно копие на всички файлове, частично – прави се резервно копие на всички променени и нови файлове след последното резервно копиране и разграничително – копират се файловете, които са променени и новосъздадени след последното пълно резервно копиране. Често се използват различни комбинации от видовете резервно копиране, за да се постигнат поставените в стратегията цели. И независимо от дефинираните приоритети и използвания вид резервно копиране (или комбинация от видове) е необходимо в стратегията за резервно копиране и възстановяване на данните в компаниите да е заложено спазването на правилото 3-2-1 за резервно копиране на данните. Неразривна част от всяка корпоративна стратегия за резервно копиране на данни трябва да бъде и изискването за задължително прилагане на периодичен външен, независим одит на защитата и резервното копиране на данните. Неправилното или частично изпълнение

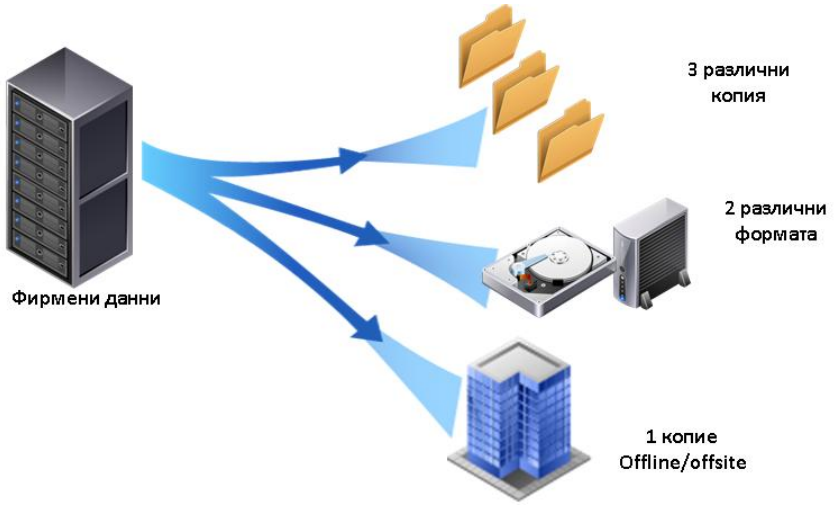
[1] Limoncelli T., Chalup S., Hogan C., The practice of cloud system administration, Volume 2, Addison-Wesley, 2014

на стратегията за резервно копиране на данните води до увеличен риск и в много случаи до загуба на данните.

Действителен случай, който подкрепя тази теза, преди няколко месеца се случи в голяма варненска компания - потребител получава писмо с прикачен файл, който му се струва, че е изпратен от данъчната администрация, записва заразен с криптовирус файл на файловия сървър в компанията, в резултат на което всички фирмени документи стават нечитаеми (криптирани). Това са файлове в разширение .docx, .xlsx, .txt, .pdf, .jpg, .rar и много други документни формати. Вирусът криптира въпросните файлове с RSA 2048, което води до загуба на всички тези файлове и антивирусният софтуер не върши работа. Данните на този потребител, следвайки общоприетото правило за резервно копиране 3-2-1, се пазят на файловия сървър, на външен диск, свързан към сървъра и на DVD дискове, записвани от време на време. Освен това се пазят и скрити копия на файловете (shadow copies) от операционната система. Оказва се, че криптовирусът е изтрил скритите копия на файловете, заразил е всички документи на файловия сървър, след това и документите на външния диск, включен към сървъра. Така единствения шанс (освен неприемливия и без никаква гаранция начин – плащане на IT рекетьорите) остават копията на дискове, които за съжаление са по-стари от един месец и потребителят загубва работата си, извършена междувременно.Такива истории, особено в последно време, се случват твърде често и са свързани най-често с пика на разпространение на подобни зловредни програми.

Този случай ни наведе на мисли за необходимост от промени, допълнения и уточнения към общоприетото правило за създаване и поддържане на резервни копия на IT ресурсите 3-2-1

Правилото 3-2-1, описано от фотографа Петер Крогх[2], представлява стратегия за резервно копиране с цел гарантирана защита от загуба на данните. Описано е като стратегия за защита на снимки, но е валидно и общоприето и за защита на данните, независимо от техния формат.



Фиг. 1 Правило 3-2-1

Правилото 3-2-1 отговаря на два въпроса: колко резервни копия на файловете трябва да се пазят и къде да се съхраняват те. Правилото гласи, че за да се осигури надеждно съхранение (и след това възможност за възстановяването им при повреда на оригиналите) на данните е необходим следния брой от копия (представени и на фигура 1):

- 3 (три) резервни копия;
- Съхранявани в 2 (два) различни физически формата за съхранение (например твърд диск, USB, магнитна лента, DVD и др.);
- Като 1 (едно) от копията трябва да се пази на място, различно от физическото място

[2] Krogh P., The DAM Book: Digital Asset Management for Photographers, O'Reilly Media, 2009, p.207

за съхранение на оригиналния файл (offsite) (в друга сграда, в друг офис на фирмата, често в банков сейф и др.) или поне офлайн.

Така, чрез посоченото в правилото съхранение на три копия на всеки един файл, се постига отказоустойчивост и надеждност.

Ще анализираме всяка една от съставящите правилото цифри. Три копия означава оригиналното копие, плюс още две копия, като всяко от тях е на различно физическо място. Или три копия, съхранявани в различни папки на един и същ диск в един компютър не удовлетворяват правилото. Неправилно е и разчитането за резервно копие на масив от дискове RAID – той няма да помогне, ако оригиналния файл е повреден или заразен с вирус. При RAID1, например, ще се повреди/зарази и файла на втория диск. До същия резултат ще доведе и репликацията, синхронизирането или автоматизираното резервно копиране на повредения/заразен файл на друг, включително и външен диск. Ако администраторът не разбере и не реагира своевременно, ще имаме две повредени/заразени копия. Криптовирусите (а и останалите зловредни програми) заразяват мигновено , и тъй като репликацията е автоматизирана, ако и резервното копиране също е автоматизирано (а в почти всички IT инфраструктури е такова), то второто копие също ще е заразено. Трите копия са абсолютен минимум и това е първото допълнение, което правим в правилото - вместо 3-2-1 копия, го променяме на минимум три копия, в минимум два формата, на минимум едно географски отдалечено място извън оригиналното.

Второто правило – съхранение в два различни физически формата, цели да намали вероятността от погиване на данните в резултат на действието на еднородна заплаха за тях – например електромагнитен импулс, вирус и други заплахи.

Третото правило се отнася до съхранението на едно от копията извън офиса, на географски отдалечено място за съхранение, без връзка с мрежата – т.е. офлайн. Така данните ще са предпазени от пожар, кражба, наводнение и други заплахи и бедствия за тях. Често се прави съхранение на носителя на данните в банков сейф и това е пример за офлайн съхранение. Важно е и отдалеченото място да е защитено от пожар. Към различните географски местоположения, възможни за реализиране на това правило, не спадат облачните решения за съхранение на данни. Те са алтернатива на резервното копиране на магнитни ленти например, но не са офлайн съхранение на резервните копия, колкото и убедителни да са доставчиците на облачни услуги.

Второто допълнение, което можем да направим към това общоприето в IT бранша правило, е да добавим, че при следване на правилото 3-2-1, съхранението на една версия на файл няма да помогне в случай на повреждане или заразяване с вирус. Необходими са различни версии чрез съхранение на по-стари резервни копия на данните. Колко стари копия да се пазят и за какъв период от време се определя от стратегията за резервно копиране в компанията, в която водещ фактор е ценността, стойността на IT ресурсите. В случай на едновременно повреждане/заразяване на всички места на съхранение на оригиналното копие на файла, той ще може да се възстанови от по-старо резервно копие и ще се загубят само промените, направени междувременно – между времето на правене на старото резервно копие и времето, в което възниква нужда от възстановяването му.

Промените, които предлагаме, са насочени към отчитане на особеностите на облачното съхранение на данни и отчитане на важността и необходимостта от пробно възстановяване на резервните копия на данните.

Първата промяна, която предлагаме, е да предложим модифициране на правилото и то да стане 4-2-1, в случай, че се разчита на услуга за резервно копиране на данните в облачна IT инфраструктура.

В облачната IT инфраструктура (правим уточнение, че трябва да става дума не за съхранение на данните в облак, а за използване на услуга за резервно копиране на данните в облачна IT инфраструктура) данните могат да бъдат загубени, както и на всяко друго място за съхранение. Не трябва да се подценяват и проблемите, свързани със сигурността на облачните решения за съхранение на данни, със срив в Интернет връзката с хранилището, срив във

услугата на доставчика на облачни решения, с по-бавното извличане на данните и не на последно място цената. Има много примери за проблеми с облачните услуги. Някои от тях не са могли да бъдат предвидени предварително - като голямото наводнение в Тайланд през 2011 година, вследствие на проливни дъждове. В Тайланд се намират повечето заводи, произвеждащи твърди дискове и повечето са наводнени и спират работа. Цените на твърдите дискове се повишават рязко, а доставките им се нарушават. В следствие на това бедствие и нарушаването на доставките, изчислителните центрове на Amazon, един от най-големите доставчици на облачни услуги, остават без необходимото оборудване и изпитват проблеми в работата си.[3]

Възможен проблем на съхранението на резервните данни в облачна IT инфраструктура са прекъсванията в услугата, която се случва дори на най-големите доставчици на облачни услуги.[4]

Резервното копиране и възстановяване на няколко терабайта не е безпроблемно, безплатно и бързо. Съхранението на данните на компанията в облачна система за съхранение е само възможно трето копие на данните от правилото за резервно копиране на данни. И като гаранция срещу проблемите на облачното резервно копиране на данните предлагаме да се коригира правилото 3-2-1 на 4-2-1, в случай, че се ползва доставчик на резервно копиране в облачна IT инфраструктура. Две от копията в този случай би трябвало да са разположени на различни облачни IT инфраструктури.

Тестването (пробното възстановяване) на резервните копия на данните е не по-малко важно от следването на правилото 3-2-1 или модификацията му 4-2-1, предлагана в настоящата разработка. Освен това, при пробното възстановяване на резервни данни е нужно и съобразяване с особеностите на тестването при различните данни и конфигурации – файлове, бази от данни... Затова предлагаме да се направи още една промяна в правилото и то да стане 3-2-1-t или 4-2-1-t при варианта с използване да облачен доставчик на услуга за резервно възстановяване на данните.

Стриктното следване на правилото за резервно копиране оскъпява данните. Принципът, който важи е, че стойността на защитата на един обект не трябва да надвишава стойността на обекта – в случая с резервното копиране – стойността на защитата на данните не трябва да надвишава стойността на данните. Ако загубата на дадени данни не е критична за бизнеса, то не е необходимо спазването на правилото за резервно копиране. Например, резервното копие на електронната поща от предишна година е възможно да се съхранява и в едно копие, ако се прецени, че стойността от загубата на тези данни няма да е толкова висока, че да се защитават по правилото 3-2-1.

В заключение стриктното спазване на правилото за резервно копиране е задължително само за данни, чиято стойност е висока и същевременно стойността на евентуалната им загуба също е висока. За останалите данни е възможно да се изпълнява правилото 3-2-1, но в някакъв негов орязан вариант, т.е. частично да се реализира, според необходимите за това средства. Важно е да се преценят и всички възможни заплахи за данните, тяхната степен на вероятност да се случат, тези възможни заплахи периодично да се оценяват отново и да се актуализират и пак да се преценява необходимостта от степента на спазване на правилото 3-2-1 – пълно или частично.

Изводи

Всеки системен администратор трябва да прави резервни копия на данните и да бъде постоянен в тази си дейност. Този принцип е валиден и за традиционна, и за виртуализирана IT инфраструктура. За да се избегне загубата на данни се създава и следва стратегия за резервно копиране и възстановяване на данните в компанията. Модифицирайки и допълвайки правилото

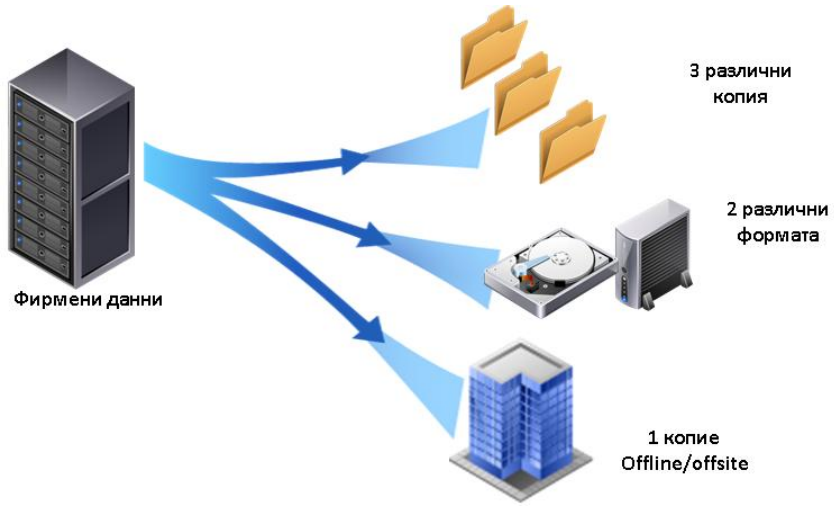
[3] Miller R., 2015, http://datacenterfrontier.com/floods-thailand-aws-supply-chain/

[4] Whittaker Z., 2013, http://www.zdnet.com/article/amazon-web-services-suffers-outage-takes-down-vine-instagram-others-with-it/

се надяваме да увеличим надеждността и отказоустойчивостта на данните, на ресурсите на компаниите. Но заедно със следването на правилото за резервно копиране на данните е свързано изискването за задължително прилагане на периодичен външен, независим одит на защитата и резервното копиране на данните. Задължително е и пробното възстановяване на данни от резервно копие и проверка дали се възстановяват позволенията им, както и тестване на повреда във възстановените файлове.

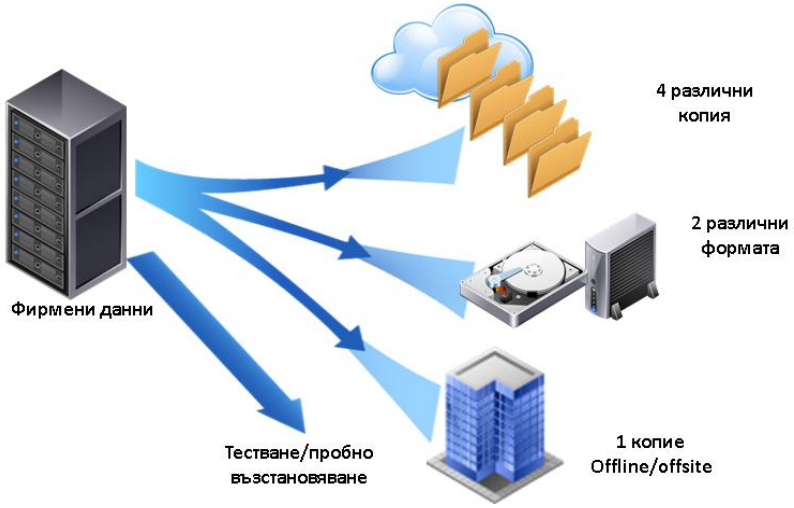
Промените, които предлагаме в правилото 3-2-1 са:

- Да се коригира правилото 3-2-1 на 4-2-1, в случай, че се ползва доставчик на резервно копиране в облачна IT инфраструктура. Две от копията в този случай би трябвало да са разположени на различни облачни IT инфраструктури;



Фиг. 2 Правило 4-2-1-t

- Предлагаме правилото да стане 3-2-1-t или 4-2-1-t при варианта с използване да облачен доставчик на услуга по резервно възстановяване на данните. Буквата t означава задължително периодично пробно, тестово възстановяване на резервни данни, съобразено и с тяхната специфика.



Фиг. 3 Правило 3-2-1-t

Допълненията, които предлагаме в правилото 3-2-1 са:

- Да се допълни правилото и да стане: за надеждно съхранение на данните са необходими минимум три копия, в минимум два формата, на минимум едно географски отдалечено място извън оригиналното;

- Данните е необходимо да се съхраняват в различни версии чрез съхранение на по-стари резервни копия.

Не всички бедствия са предсказуеми и не срещу всички можем да организираме защитни действия и противодействие, но комбинацията на спазването на правилото за резервно копиране, задължителното пробно възстановяване и IT одита са гаранцията за здравето на данните на компаниите.

Използвана литература:

1. Limoncelli T., Chalup S., Hogan C., The practice of cloud system administration, Volume 2, Addison-Wesley, 2014
2. Krogh P., The DAM Book: Digital Asset Management for Photographers, O'Reilly Media, 2009
3. Miller R., 2015, http://datacenterfrontier.com/floods-thailand-aws-supply-chain/
4. Whittaker Z., 2013, http://www.zdnet.com/article/amazon-web-services-suffers-outage-takes-down-vine-instagram-others-with-it/

За контакти:

Ас. Михаил Радев Миланов
Икономически университет – Варна
E-mail: radev@ue-varna.bg