Резервное копирование как основной компонент информационной безопасности

Обзор методов и технологий резервного копирования от компании COMMVAULT, дополняющих решения по информационной безопасности в свете современных угроз.

Евгений Пухов – технический консультант, COMMVAULT Россия и СНГ.

Как справиться с растущими рисками с сфере ИТ? Как предотвратить кражу информации? Как уберечься от вредоносного ПО и Ransomware атак?

Эксперты выделяют две основные причины существования и распространения вирусных угроз: уязвимости в программном обеспечении и человеческий фактор.

Уязвимости везде – никто не может знать наперед, какие «дыры» остались в используемых вами операционных системах, приложениях, протоколах. Более того, их количество растет, так как в погоне за функционалом и скоростью вывода новых технологий на рынок, производители ПО сознательно и несознательно порождают новые уязвимости и недокументированные возможности. Процесс разработки нового вредоносного кода в этом случае – это исключительно вопрос времени. Соответственно, не может существовать надежного антивируса или сетевого экрана, способного предотвратить ВСЕ возможные атаки. Более того, в последнее время сами антивирусы становятся целью атак.

Вторая причина распространения вредоносного кода – человеческий фактор. Как показывает практика, виноваты обычные пользователи ПК, которые в силу невнимательности и недостатка компьютерной грамотности подвергают свои компьютеры угрозам, которые затем распространяются на другие ресурсы в компании. Более того, очень часто на рабочих компьютерах оказывается гораздо больше критичной для бизнеса и конфиденциальной информации, чем на файловом сервере компании – эта организационная проблема, к сожалению, по-прежнему актуальна...

Вот и получается, что на сегодняшний день на рынке существует единственный способ защиты данных, обеспечивающий их максимальную сохранность. Метод, который проще и надежнее всех прочих возможных инструментов информационной безопасности – резервное копирование. Конечно, справедливо это в том случае, если следовать довольно простым рекомендациям, часть из которых приведена в этой статье.

Последнее время мы стараемся даже не употреблять термин «резервное копирование», мы говорим, скорее, «управление копиями данных». Связано это с тем, что эти самые копии используются не только в случае полной или частичной потери данных: они используются для целей разработки и тестирования, для задач миграции на другие платформы и БД, для целей DR и репликации.

Если отбросить весь прочий функционал (аналитические, поисковые возможности, интеграцию со сторонним ПО), Commvault – это горизонтально масштабируемая платформа хранения «вторичных» данных в виде этих самых копий и различных архивов. Важно отметить, что Commvault не управляет продуктивными приложениями и системами хранения, Commvault лишь создает правильный интерфейс связи первичных и вторичных данных, сохраняя целостность и прозрачность доступа к информации.

Итак, какие принципы должны обеспечиваться, чтобы хранение данных было максимально защищенным, и что предлагает Commvault:

- ***ролевая модель администрирования.*** Нужно дать ровно тот минимальный уровень доступа, который позволит выполнять конкретные функции ИТ специалисту. Очень многие забывают об этом, считая Role based Access Control (RBAC) от Commvault слишком сложным, но так это и задумано, чтобы можно было создавать более грануляр-ные, более тонкие права. Например, по одному и тому же объекту (пусть будет файловый сервер) можно создать порядка 10–20 разных ролей: возможность выполнять резервные копии, восстановление, просматривать содержимое, выполнять мониторинг, создавать системные уведомления в случае достижения каких-то параметров и т.п. Важно, что Commvault позволяет разделить пользователей на тех, кто занимается непосредственно ***защитой и управлением данных,*** кто занимается ***мониторингом,*** и тех, кто занимается вопросами ***информационной безопасности***. Это и есть суть ролей RBAC. Естественно, что службы безопасности в крупных компаниях имеют на вооружении огромное количество инструментов, помимо наших, однако возможности Commvault по мониторингу ресурсов, журналированию всех действий с данными им всегда интересны;
- ***ограничение видимости ресурсов.*** Если компьютер физически не подключен к интернету, вредонос, очевидно, его никогда не атакует. Очень простые рекомендации, которые мы даем на любом серьезном проекте по внедрению систем защиты данных: ограничивайте видимость ресурсов. Вы хотите, чтобы в случае падения вашей виртуальной платформы вы смогли поднять ее из резервной копии? – Тогда хотя бы не храните копии на тех же системах хранения вместе с продуктивными данными. Commvault устанавливается на любое x86-железо и не требует специфических аппаратных средств, поэтому высок соблазн после того, как выполнено пилотное внедрение, все так и оставить в продуктиве. Мы настаиваем, чтобы инфраструктура хранения резервных копий была физически и логически изолирована от продуктивных систем. В идеале – также физически разделять трафик резервного копирования, но, к сожалению, это не всегда возможно.

В этом контексте важно упомянуть шифрование. Рекомендации по шифрованию продуктивных бизнес-критичных систем Commvault не дает. Вопрос нужно ли шифровать резервные

копии? Шифрование не лекарство от всех бед, так как злоумышленник может поставить цель не прочитать информацию, а полностью ее уничтожить. Мы считаем, что шифрование резервных копий и архивов оправдано в том случае, если ограничение видимости и разделение ролей доступа сделать невозможно из-за особенностей ИТ-среды (например, в случае, если кассеты с резервными копиями требуется перевозить между локациями);

– ***создавайте копии данных на разных носителях.*** Диск – быстр и оперативен, но потребляет электроэнергию, ломается и потенциально подвержен вредоносной атаке. Лента – дешевле и не может быть атакована никаким вирусом в принципе. Любой носитель имеет плюсы и минусы. Чтобы "защита была защищенной", нужно подумать о создании многоуровневой системы хранения данных. Не забываем про Cloud. Несмотря на ограниченную распространенность в России, ведущие мировые cloud-провайдеры имеют систему защиты, которую не могут себе позволить средние компании. Поэтому создание второй или третьей копии данных в облаке – реальная альтернатива созданию собственного не зависимого от продуктива изолированного периметра. Если речь идет о зарубежных провайдерах, то нужно прорабатывать вопрос шифрования данных и, конечно, не забыть о защите персональных данных в соответствии с 152-ФЗ;

– ***защита «конечных точек» – рабочих компьютеров пользователей***. Как правило, сам ЦОД надежно защищен, Ransomware ВСЕГДА (по крайней, мере по официальной статистике) пролезает через конечные рабочие станции пользователей, которые имеют доступ к данным в этом ЦОД и одновременно имеют, например, доступ к электронной почте. Поэтому раннее обнаружение нужно начинать с рабочих мест.

  Commvault противодействует Ransomware, используя технологию *Honeypot trap*. В каждый из защищаемых копьютеров размещается специальный файл в таком расположении, что никто не будет его трогать, включая специализированное ПО. Момент обращения к такому файлу (особенно, если это событие произошло не на единичном компьютере), приведет к выполнению заранее предопределенных действий: это может быть как отсылка уведомлений, так и отработка определенного сценария. Помимо этого, мы можем регистрировать изменение профиля доступа к общим файловым ресурсам (который вдруг стал сильно отличаться от повседневного) или высокий процент изменений данных по сравнению с последним бэкапом – высокий процент изменений может означать начало работы вируса-шифровальщика. Это дает возможность увидеть деструктивные процессы до того, как они заявят о себе активно и начнут распространяться по сети.

  Нам часто говорят, что рабочие места сотрудников не предназначены для хранения файлов и поэтому смысла заниматься защитой десктопов нет, т.к. проблема решена организационно. Что произойдет, если сотрудник нарушит эти требования? Как компания узнает о том, что критически важная и конфиденциальная информация попала на компьютер, который , например, был утерян. В том и дело, что технологии по защите данных и резервного копирования направлены в данном случае на задачи информационной безопасности;

– ***используйте DR для достижения высоких SLA в терминах RTO/RPO.*** Многие спрашивают о том, какие скорости копирования и восстановления гарантирует Commvault. Мы лишь запускаем процессы – даем команду приложениям, системам хранения, инициируем передачу данных. Скорость зависит не от Commvault, а от всего остального. Общая практика – если ваше приложение требует RTO/RPO меньше, чем один час, используйте DR на уровне приложений с репликацией данных. Не стоит забывать, что если сделана репликация данных для целей защиты данных, то после того, как вирус-шифровальщик подвердит данные на источнике, ваша система синхронизации данных автоматически это отреплицирует во вторичный ресурс. Поэтому, даже если на вооружении стоит мощная и дорогая DR-стратегия, про старые добрые резервные копии не забывайте.

Про обновления Commvault: изменения идут постоянно, это и новый функционал, исправления ошибок и конечно же поддержка всех самых современных ОС и приложений. Удобнее всего следить за обновлениями на открытом ресурсе с документацией: *http://documentation.commvault.com/commvault/v11/article?p=whats_new/c_whats_new_overview.htm*. Все обновления удобно отсортированы по дате выхода и типу.

Довольно много обновлений по части поддержки облачных сред: помимо возможности создавать копии данных в облачных ресурсах, мы научились делать наоборот – создавать РК облачных сервисов, таких как Google Mail, Google Drive, Amazon S3, Microsoft Onedrive, Office 365 Exchange online. Полезный функционал для малых компаний, которые не имеют своего продуктивного почтового или файлового сервера, однако предпочли бы иметь локальную копию облачных данных (например, для задач соответствия требованиям регуляторов).

Появился многопоточный параллельный бэкап распределенных ФС и DWH: GPFS, Pivotal Greenplum, Hadoop. Появилась возможность резервировать Apache Cassandra.

Получило продолжение развитие веб-административной консоли, если раньше в ней можно было выполнять только «бытовые» задачи – резервное копирование и восстановление, то теперь возможно настраивать политики хранения, права доступа, работать над более тонкими настройками защиты БД и приложений.

Интересные добавления по задачам по миграции данных и приложений: с помощью Commvault можно переносить приложения и БД из локального ЦОД в облако, делать конверсию физических серверов в виртуальные машины (в том числе физический Linux -> Hyper V).

Появилась возможность прямого доступа к хранилищу Commvault Contentstore по протоколу NFS. Теперь для выполнения РК можно вообще не использовать агенты, и выполнять защиту данных «родными» средствами приложений, храня резервные копии на NFS. Запуск этих процессов можно инициировать из Commvault, как и обычные задания.

В заключение хотелось бы еще раз отметить, что, несмотря на обилие современных технологий по противодействию атакам, реализация консервативных методик защиты данных, таких как резервное копирование должна проводиться в первую очередь.

Евгений Пухов,
COMMVAULT Россия и СНГ.

Gartner: Commvault лидирует на рынке РКВ

Август 2017 г. — Компания Commvault (NASDAQ: CVLT), глобальный лидер в защите, резервном копировании, восстановлении и архивировании корпоративных данных и сопутствующих облачных технологиях, объявила, что аналитическое агентство Gartner, Inc. поместило ее в квадрант «Лидеры» недавно опубликованного «Магического Квадранта решений корпоративного класса для резервного копирования и восстановления» (Magic Quadrant for Data Center Backup and Recovery Solutions)[1]. Среди компаний, включенных в квадрант «Лидеры», у Commvault самая высокая оценка «полноты видения» (completeness of vision).

Согласно отчету, «Gartner анализирует и оценивает ведущих поставщиков решений резервного копирования для датацентров, которые предлагают различные традиционные и инновационные средства обеспечения высокой доступности данных».

«Высокая оценка Gartner, которую мы получаем седьмой год подряд – это доказательство наших инноваций и уникального сервиса для клиентов. Это очень важная новость как для компании Commvault, так и для ее заказчиков и партнеров, – подчеркнул Н. Роберт Хаммер *(N. Robert Hammer)*, председатель правления, президент и исполнительный директор Commvault. – Мы считаем, что наши простые и удобные для работы решения на базе нового полнофункционального пользовательского интерфейса, привлекательной модели ценообразования и различных опций на основе мощной платформы Commvault Data Platform укрепляют лидирующие позиции нашей компании на рынке резервного копирования. Мы уверены, лучшая в индустрии автоматизация, переносимость данных и уникальная поддержка облачных вычислений сделали Commvault ведущим поставщиком решений для предприятий, которые переходят к облачным сервисам. Хочу поблагодарить наших сотрудников,