Защита от вирусов-вымогателей

Устройства Veritas NetBackup™ Appliance

Использование программного обеспечения Veritas NetBackup и устройств NetBackup Appliance для защиты от вирусов-вымогателей и ликвидации последствий атак.

VERITAS

Истина в информации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

КРАТКАЯ АННОТАЦИЯ

Вирусы-вымогатели и их атаки — очень серьезная проблема для крупных организаций. Направленный фишинг действительно работает. Вирусы-вымогатели — это большой бизнес, и злоумышленники неустанно работают над новыми, нестандартными методами проникновения в корпоративные сети и ИТ-среды с целью захвата данных и получения выкупа. В этих условиях на первый план выходит способность противостоять атакам и ликвидировать их последствия в любых масштабах. Крупным предприятиям также рекомендуется пользоваться возможностями облака и разработать гибридный подход, опирающийся на локальную инфраструктуру в связке с облачными услугами нескольких поставщиков.

Устройства NetBackup Appliance представляют собой простые, высокопроизводительные и защищенные решения для резервного копирования данных. Как комплексные решения для защиты данных, устройства NetBackup Appliance хорошо подходят для защиты от атак, направленных на инфраструктуру резервного копирования и восстановления данных, а также для быстрого восстановления производственных сред после таких атак. Благодаря этому организации получают возможность полностью сконцентрироваться на своем профильном бизнесе, не отвлекаясь на обслуживание инфраструктуры. Устройства NetBackup Appliance разработаны с целью объединить лучшие инструменты защиты и восстановления данных с механизмами интеграции с облачными услугами разных поставщиков.

ПРЕДМЕТ ИССЛЕДОВАНИЯ

Настоящий документ содержит общую информацию о проблеме вирусов-вымогателей и внутренних вредителей, описывает принципы работы вирусов-вымогателей, а также дает рекомендации по защите и ликвидации последствий атак с помощью устройств Veritas NetBackup Appliance. Хотя в данном документе приведены общие рекомендации и описаны передовые практики, его не следует рассматривать в качестве исчерпывающего источника информации или руководства по внедрению.

ЦЕЛЕВАЯ АУДИТОРИЯ

Этот документ предназначен для клиентов, партнеров и сотрудников Veritas, заинтересованных в применении устройств NetBackup Appliance для защиты от кибератак, способных необратимо уничтожить или зашифровать данные, а также для ликвидации последствий таких атак.

ЧТО ПРЕДСТАВЛЯЮТ СОБОЙ ВИРУСЫ-ВЫМОГАТЕЛИ?

Вредоносными программами называют программы, созданные с целью нарушения работоспособности компьютера или удаления данных. Они подразделяются на несколько типов: вирусы, троянские кони, черви, программы-шпионы и рекламные программы. Эта публикация не о них. Вирусы-вымогатели — это особый тип вредоносных программ. Они уникальны тем, что пытаются блокировать доступ к компьютеру или зашифровать данные на нем. Пользуясь уязвимостями операционной системы, вирусы-вымогатели могут пытаться заразить другие компьютеры. Затем они требуют выкуп за восстановление доступа к системе или расшифровку данных. Киберпреступники часто находятся за тысячи километров в далеких странах и требуют уплаты выкупа в форме, не позволяющей идентифицировать получателя и вернуть уплаченные средства. Это могут быть биткойны и другие электронные валюты либо номера предоплаченных карт, например Apple iTunes, Google Play или т. п., которыми можно воспользоваться для получения наличных или покупки товаров и услуг. Зачастую уплата выкупа не оставляет цифрового следа и не позволяет найти преступников, не говоря уже о том, чтобы вернуть заплаченные деньги. Вдобавок к этому нет никакой гарантии, что преступники расшифруют данные после получения выкупа. В статье *Нерассказанная история о NotPetya — самой разрушительной кибератаке в истории* говорится об атаке на компанию Maersk, которая нанесла ущерб на сумму свыше 10 миллиардов долларов.

ВИРУСЫ-ВЫМОГАТЕЛИ И ШИФРОВАНИЕ

Вирусы-вымогатели используют два вида шифрования данных. Когда вирус пользуется первым видом шифрования, у него есть ключ, позволяющий расшифровать данные, и преступники требуют выкуп за этот ключ. У второго вида шифрования нет ключей. Этот вид шифрования особенно опасен, потому что для шифрования каждого отдельно взятого файла создается уникальный случайный ключ, который нигде не сохраняется. Даже если заплатить выкуп, расшифровать данные не получится. Фактически данные оказываются недоступными, расшифровать файлы становится невозможно, и информацию можно восстановить только из резервной копии.

Вирусы-вымогатели могут попасть в организацию разными путями. Это может быть направленный фишинг, вредоносный сайт или зараженный USB-накопитель.

ВНУТРЕННИЕ ВРЕДИТЕЛИ

Хотя в данном случае речь не идет о вирусах-вымогателях и вредоносных программах, внутренние вредители создают похожую угрозу для важнейших данных компании. Речь идет о ситуациях, когда лицо, которому предоставлен доступ к конфиденциальным данным компании, удаляет эти данные, шифрует их или перемещает куда-либо, а затем требует выкуп. Атаки внутренних вредителей особенно неприятны тем, что злоумышленнику могут не потребоваться ни вредоносные программы, ни шифрование. Он может просто хотеть нанести ущерб, не требуя выкупа.

ВИРУСЫ-ВЫМОГАТЕЛИ В НОВОСТЯХ

Угроза атаки вирусов-вымогателей существует всегда и становится только серьезнее, потому что подобные преступления могут совершаться из любой точки планеты, а киберпреступникам легко скрыть свои цифровые и финансовые следы. Новости о новых жертвах таких атак появляются с завидной регулярностью. Следующие статьи посвящены вирусам-вымогателям, использующим шифрование.

- Нерассказанная история о NotPetya — самой разрушительной кибератаке в истории (ссылка)
- Городской совет Атланты тратит 2,6 миллиона долларов на ликвидацию последствий атаки вируса-вымогателя, требовавшего 52 000 $ (ссылка)
- Шотландский пивоваренный завод ликвидирует последствия атаки вируса-вымогателя (ссылка)

КРИПТОВАЛЮТА И ПЕРЕГОВОРЫ С ВЫМОГАТЕЛЯМИ

Отдельного упоминания заслуживает то, что уже появились компании, предлагающие услуги по ведению переговоров с вымогателями криптовалюты для уменьшения суммы выкупа. Некоторые организации даже решили приобрести и хранить небольшое количество криптовалюты на случай, если они станут жертвами атаки вируса-вымогателя. Даже на этих примерах видно, насколько серьезна проблема вирусов-вымогателей.

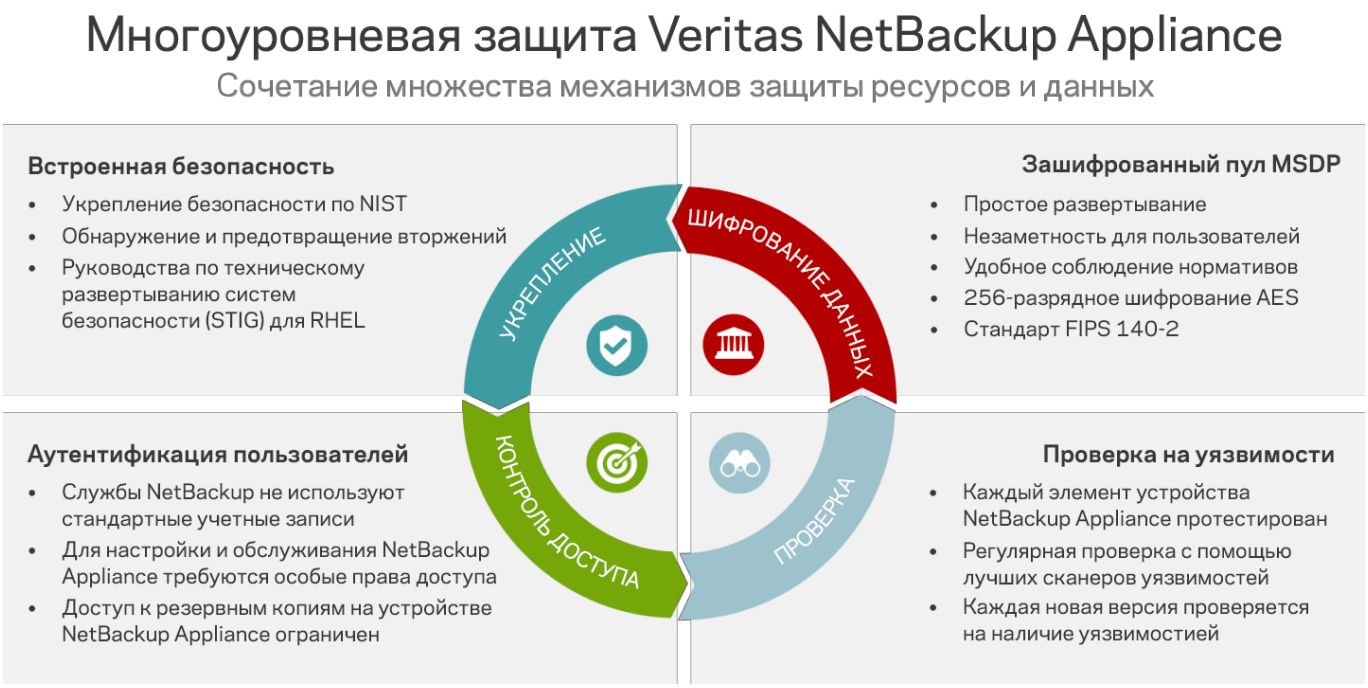
- Услуги по ведению переговоров с киберпреступниками, вымогающими биткойны (ссылка)

Как компаниям защититься от кибератак и ликвидировать их последствия, если атаки окажутся успешными?

ДОСТОИНСТВА УСТРОЙСТВ NETBACKUP APPLIANCE

МНОГОУРОВНЕВАЯ ЗАЩИТА

Устройства NetBackup Appliance содержат оптимизированную версию NetBackup и интегрированные многоуровневые механизмы безопасности, помогающие обеспечить максимальную защиту от вирусов-вымогателей и других форм киберпреступности.



РАЗРАБОТАНО СПЕЦИАЛЬНО ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководства по техническому развертыванию систем безопасности (STIG) разработаны на основе правил американского Управления оборонных информационных систем (DISA). Они содержат технические рекомендации по повышению безопасности информационных систем и программного обеспечения, помогающие предотвратить атаки на компьютеры. Процесс реализации требований STIG часто называют укреплением безопасности. Механизмы STIG интегрированы в операционную систему устройств NetBackup Appliance. Федеральное правительство США требует включения STIG на устройствах, используемых в правительственных системах. Поддержка STIG включается из командной строки, и после включения ее нельзя отключить.

Инструкции по включению приведены в Руководстве по обеспечению безопасности устройств Veritas NetBackup Appliance.

SYMANTEC DATA CENTER SECURITY

Решение Symantec Data Center Security (SDCS) встроено во все устройства NetBackup. Оно автоматически запускается при включении устройства и не требует обслуживания. Решение SDCS располагает лучшими в отрасли встроенными средствами предотвращения и обнаружения вторжений и работает без агентов. Оно не требует установки, настройки и специализированных знаний для начала работы. SDCS может предотвратить большинство атак вирусов-вымогателей. Оно обеспечивает очень надежную защиту от атак, направленных на шифрование дисков, и способно помешать уничтожению и шифрованию резервных копий файлов.

ЗАШИФРОВАННЫЙ ПУЛ MSDP

Для минимизации нагрузки на сеть, инфраструктуру и подсистему хранения устройства NetBackup Appliance оснащаются встроенными средствами дедупликации. Когда клиенты NetBackup создают резервные копии данных в устройстве NetBackup Appliance, данные помещаются в пул дедупликации сервера резервного копирования (MSDP). После дедупликации они могут шифроваться для дополнительной безопасности. Данные хранятся в зашифрованном виде и могут быть прочитаны только с помощью NetBackup. Пул MSDP осуществляет шифрование по 256-разрядному стандарту AES и обеспечивает выполнение требований американского федерального стандарта обработки информации FIPS PUB 140-2 по отношению к данным, записываемым на носители. По умолчанию поддержка FIPS не включена; ее необходимо включить вручную в дополнение к MSDP. Для доступа к зашифрованным данным в MSDP требуется уникальный ключ; внутренние ключи шифрования сегментов генерируются автоматически.

Следует отметить, что вирусы-вымогатели и MSDP пользуются разными видами шифрования. Шифрование MSDP не влияет на коэффициент дедупликации, в отличие от шифрования вирусов-вымогателей. Дополнительные сведения об этом важном различии приведены ниже в разделе, посвященном NetBackup OpsCenter.

Подробную информацию о MSDP и шифровании MSDP можно найти в Руководстве по дедупликации Veritas NetBackup.

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Для ограничения доступа к ресурсам устройства применяется контроль доступа на основе ролей (RBAC). Настраивать устройство NetBackup и управлять им могут только пользователи, которым назначена роль администратора.

В отличие от многих других продуктов для резервного копирования, NetBackup не пользуется учетными записями обычных пользователей для доступа к образам резервных копий. Службы NetBackup работают под управлением неинтерактивных учетных записей. Такие учетные записи не используются для проверки электронной почты и доступа к внешним веб-сайтам, и поэтому они заведомо более безопасны.

ПРОВЕРКА НА УЯЗВИМОСТИ

Устройства NetBackup Appliance изначально разрабатывались с прицелом на безопасность. Все компоненты устройства, включая адаптированную операционную систему Linux и базовое приложение NetBackup, проверяются на наличие уязвимостей с помощью стандартных и расширенных инструментов безопасности. Необязательные пакеты удалены с устройства, чтобы не создавать лишних возможностей для проведения атаки. Эти меры помогают минимизировать риск несанкционированного доступа и потери данных.

Все версии программного и аппаратного обеспечения устройств NetBackup перед выпуском проверяются на наличие уязвимостей. В зависимости от серьезности обнаруженной проблемы, Veritas выпускает оперативное исправление или устраняет проблему в следующей версии продукта. Для уменьшения рисков, исходящих от известных угроз, Veritas регулярно обновляет пакеты и модули сторонних разработчиков, используемые в продукте.

Каждая версия тестируется в три независимых этапа с помощью новейших средств разработки ПО.

- Статический анализ кода

  Программный код анализируется на наличие дефектов во время разработки с помощью таких инструментов, как FindBugs™, PMD и Coverity®.

- Проверка среды выполнения на уязвимости

  Все версии кода среды выполнения проверяются несколькими сканерами уязвимостей, такими как Nessus®, Qualsys®, Trustwave® и OpenSCAP

- Независимое тестирование на проникновение

  Тестирование интерфейсов устройства на возможность проникновения выполняется сторонними

компаниями. Veritas регулярно обновляет пакеты и модули сторонних разработчиков в рамках плановых циклов обслуживания программного обеспечения.

Важная информация: хотя Veritas пользуется множеством инструментов в ходе разработки программного обеспечения, компания не дает никаких рекомендаций в отношении этих инструментов.

ЗАЩИТА ОТ ВИРУСОВ-ВЫМОГАТЕЛЕЙ И ВНУТРЕННИХ ВРЕДИТЕЛЕЙ

ПРЕДОТВРАЩЕНИЕ, ОБНАРУЖЕНИЕ И ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ

Защиту от вредоносных действий можно разделить на три стадии: профилактику, обнаружение и ликвидацию последствий. Кибератаки — испытание на прочность для механизмов защиты организации на всех трех стадиях. Лучшая стратегия заключается в развертывании всех имеющихся средств защиты на всех трех стадиях параллельно с отработкой процедур ликвидации последствий на случай, если атака окажется успешной.

ПРЕДОТВРАЩЕНИЕ

На стадии *предотвращения* вы стремитесь воспрепятствовать доступу злоумышленников и вредоносных программ в ваши системы и сеть. Здесь возможны разные стратегии. Одна из важнейших мер заключается в том, чтобы администраторы всегда знали обо всех новых исправлениях сетей и компьютерных систем и поддерживали их актуальность. Вирусы-вымогатели часто пользуются уязвимостями систем, в которых установлены не все актуальные исправления. Также для минимизации угроз рекомендуется реализовать почти все или все следующие дополнительные стратегии, хотя и это — не исчерпывающий список:

- ограничение физического доступа к производственным системам обработки данных и в особенности к системам резервного копирования и восстановления;
- ограничение доступа к сети путем установки брандмауэров и минимизации использования портов;
- развертывание системы авторизации пользователей и управления доступом на основе ролей;
- фильтрация URL и адресов электронной почты;
- отработка процедур ликвидации последствий атак;
- обучение пользователей основам безопасности.

Организациям необходимо разработать SLA (соглашения об уровне обслуживания), устанавливающие перечень и стандарт предоставления ИТ-услуг конечным пользователям. В частности, в SLA должны быть оговорены такие характеристики, как RPO (целевая точка восстановления) и RTO (целевое время восстановления). Требования к RPO и RTO часто зависят от конкретной категории данных и могут быть разными для баз данных, виртуальных машин, домашних каталогов пользователей и т. д. Выбор оптимальных средств резервного копирования и восстановления данных среди всего многообразия вариантов зависит от параметров RPO и RTO. Важная составляющая стадии предотвращения заключается в заблаговременном описании стадии *ликвидации последствий* и непрерывной отработке соответствующих процедур. Стадия ликвидации последствий обсуждается ниже.

ОБНАРУЖЕНИЕ

Стадия *обнаружения* призвана обеспечить быстрое выявление подозрительных действий. Подобно стадии предотвращения, стадия обнаружения требует комплексного подхода. Для всесторонней защиты необходимо принять практически все или все нижеперечисленные меры:

- защита пользовательских конечных систем;
- антивирусная защита корпоративного класса для серверов;

- обнаружение вторжений;
- обнаружение известных вредоносных программ;
- мониторинг сетевых портов;
- централизованное ведение журналов для сопоставления событий;
- выявление шаблонов данных (см. информацию об OpsCenter ниже).

Быстрое обнаружение вредоносных действий помогает остановить или заблокировать атаку до того, как она перекинется на другие системы и нанесет еще больший ущерб. Зараженные системы необходимо немедленно изолировать. Затем нужно ликвидировать угрозу, а после этого — восстановить работоспособность систем.

ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ

Если угрозу не удастся предотвратить и о ней станет известно лишь на стадии обнаружения, последним рубежом обороны будет стадия *ликвидации последствий*, направленная на быстрое и надежное восстановление данных. На этой стадии активно используются процедуры восстановления и программное обеспечение для резервного копирования и восстановления данных. Данные нужно восстанавливать быстро. Наличие резервных копий данных на магнитной ленте во внешнем хранилище, или *воздушного зазора*, также входит в комплекс мер защиты на стадии ликвидации последствий, потому что именно эти копии могут потребоваться для восстановления.

ПРЕДОТВРАЩЕНИЕ: КАК ПРЕДОТВРАТИТЬ ИЛИ ОГРАНИЧИТЬ ПОТЕРЮ ДАННЫХ

Помимо надежно защищенного устройства резервного копирования и восстановления данных, для максимальной безопасности резервных копий необходимо пользоваться дополнительными средствами. В этом разделе обсуждаются дополнительные стратегии предотвращения потери данных, которыми можно пользоваться при настройке сред резервного копирования, а также дополнительные инструменты для стадий *предотвращения* и *обнаружения*.

ПОВЫШЕНИЕ НАДЕЖНОСТИ ПРЕДОТВРАЩЕНИЯ АТАК ВИРУСОВ-ВЫМОГАТЕЛЕЙ

Для дополнительной защиты данных от атак следует создавать дополнительные резервные копии данных и хранить их на носителях другого типа во внешнем хранилище. Эти шаги помогают защитить все данные от потери.

ПРАВИЛО 3-2-1

Компьютерная команда экстренной готовности США (US-CERT) разработала документ под названием *Варианты резервного копирования данных* для широкого круга домашних и профессиональных пользователей компьютеров. В этом документе всем пользователям компьютеров рекомендуется соблюдать правила «3-2-1» для защиты своих данных. Соблюдение этих простых правил помогает лучше защитить данные за счет увеличения шанса успешного восстановления. Правила звучат так:

3. Храните 3 экземпляра важных данных: 1 основной и 2 резервных
2. Храните данные на 2 разных видах носителей для защиты от разных опасностей.
1. Храните 1 экземпляр в другом месте (например, за пределами офиса).

Устройства Veritas NetBackup Appliance дают администраторам удобную возможность следовать этим рекомендациям: они поддерживают разные виды носителей, копирование во внешние хранилища (включая облака и удаленные площадки) и обслуживание нескольких резервных копий данных.

ВНЕШНИЕ ХРАНИЛИЩА И ВОЗДУШНЫЙ ЗАЗОР

Действия вирусов-вымогателей и внутренних вредителей могут распространиться по сети с первого атакованного

компьютера на другие системы, включая важнейшие серверы резервного копирования. Могут быть уничтожены даже резервные копии и метаданные, и в результате не останется ни одной точки восстановления, если не будут развернуты и активно задействованы средства безопасности. Внутренние вредители, способные получить доступ к производственным системам и системам резервного копирования, могут лично позаботиться об этом. При наличии достаточных прав доступа и дыр в защите разъяренные и целеустремленные внутренние вредители могут провести чрезвычайно разрушительные инсайдерские атаки. Они могут удалить каждый бит данных в каждой доступной им системе без малейшей возможности восстановления. Иногда спасением становится какой-нибудь последний сервер или том, который был выключен или недоступен в момент атаки и на котором осталась последняя недоступная злоумышленникам копия данных.

Администраторы резервного копирования, заинтересованные в максимально надежной защите резервных копий, должны позаботиться о хранении данных во внешних хранилищах и создании воздушных зазоров для важнейшей информации. У вредоносных программ, вирусов-вымогателей и внутренних вредителей может не быть доступа к удаленным системам, в которых хранятся копии данных, и возможности преодолеть воздушные зазоры.

Размещение резервных копий во внешних хранилищах — один из лучших способов хранения нескольких экземпляров данных и выполнения рекомендаций US-CERN. Встроенные функции репликации NetBackup позволяют обслуживать более трех экземпляров данных в более чем трех хранилищах на носителях разных типов. Существуют два основных способа размещения данных во внешних хранилищах. Первый способ заключается в репликации данных в другие системы по глобальной сети. Второй способ — в физическом перемещении носителей из одного хранилища в другое. При репликации сохраняется сетевой доступ к копии данных, и вредоносная программа или вредитель теоретически все же могут получить доступ к ней.

При настройке репликации пользователи устройства NetBackup Appliance и администраторы могут создать дополнительный уровень защиты. При репликации данных на другие устройства NetBackup и в другие домены NetBackup можно по-другому настроить защиту устройств-приемников, лишив администраторов исходных систем доступа к копии данных.

Для максимальной защиты необходимо полностью запретить доступ к резервным копиям и физически исключить их доступность. Воздушным зазором называется ситуация, когда доступ к резервной копии данных из производственной сети физически невозможен. В качестве дополнительной меры безопасности необходимо периодически проводить контрольное восстановление данных в изолированной среде, чтобы убедиться, что данные находятся в сохранности, а процедура восстановления работает. Устройства NetBackup поддерживают обслуживание резервных копий в других хранилищах и создание воздушного зазора путем записи данных на магнитную ленту.

NetBackup на магнитной ленте

Самый распространенный способ создания воздушного зазора заключается в записи резервной копии на магнитную ленту и хранении магнитной ленты в другом хранилище. В результате у вирусов-вымогателей пропадает физическая возможность получить доступ к резервным копиям данных, что обеспечивает дополнительную безопасность. Устройства NetBackup поддерживают библиотеки магнитных лент.

Храните на магнитной ленте дополнительную копию важнейших данных. Рекомендуется регулярно создавать резервные копии каталогов NetBackup на магнитной ленте для их защиты. Если каталоги NetBackup станут недоступны в результате атаки вируса-вымогателя, их нужно будет реконструировать. Для этого системе NetBackup потребуется считать все резервные копии со всех носителей. Этот дополнительный шаг на этапе ликвидации последствий значительно замедлит восстановление работоспособности систем. По этой причине рекомендуется хранить резервные копии каталогов NetBackup на магнитной ленте на случай, если их тоже потребуется восстановить.

Если у злоумышленников будет доступ к магнитной ленте, они смогут похитить и даже уничтожить ее. Кроме того, магнитная лента должна храниться в условиях, исключающих повреждение носителей. Если вы создаете резервные

копии на магнитной ленте, храните магнитную ленту на отдельной защищенной площадке с контролем параметров окружающей среды.

Важно помнить о том, что применение магнитной ленты увеличивает длительность операций резервного копирования и восстановления данных, и в SLA должно учитываться дополнительное время, которое может потребоваться на восстановление.

Дополнительные сведения о подключении библиотек магнитных лент к устройствам NetBackup приведены в Руководстве по применению устройств Veritas NetBackup Appliance в сетях Fibre Channel.

Хранилище AWS Glacier в качестве устройства WORM

Устройства NetBackup работают с облачными хранилищами данных Amazon Web Services (AWS), Microsoft Azure и OpenStack Swift через API. Они также поддерживают WORM-накопители (однократная запись, многократное чтение) службы AWS Glacier с применением политик блокирования хранилищ AWS.

Хотя *неизменяемые* хранилища разрабатывались для выполнения нормативных требований, они могут быть очень полезны в качестве дополнительной меры защиты от вирусов-вымогателей. После того как данные записаны в неизменяемую систему хранения, их нельзя ни удалить, ни изменить. Помимо производственных систем и данных, важнейшие системы резервного копирования и носители резервных копий могут быть уязвимы для определенных видов атак вирусов-вымогателей и внутренних вредителей. Хранение резервных копий важнейших данных в неизменяемом хранилище значительно повышает их безопасность.

Администраторы могут создать хранилища в облаке AWS с помощью службы Glacier и политик блокирования Amazon. Затем можно настроить устройство NetBackup Appliance таким образом, чтобы резервные копии создавались с *классом хранения* GLACIER_VAULT, и таким образом превратить его в WORM-накопитель.

Администраторы должны помнить об особенностях AWS Glacier, в том числе в случае применения этой службы в качестве WORM-носителя. Во-первых, в силу характера самого хранилища восстановление данных из AWS Glacier происходит медленнее, чем с других носителей. Кроме того, поскольку данные будут храниться дольше и удаляться реже, может потребоваться значительная емкость, что потребует дополнительных расходов.

Дополнительные сведения о настройке и эксплуатации хранилища в AWS Glacier приведены в Руководстве администратора Veritas NetBackup в облаке.

Создание дополнительного уровня хранения данных в облаке с помощью устройства NetBackup Cloud Catalyst

NetBackup CloudCatalyst пользуется технологией дедупликации MSDP для загрузки дедуплицированных данных в облако. Данные загружаются сервером облачного хранилища MSDP, поддерживающим CloudCatalyst, который сначала накапливает данные в локальном кэше, а затем выгружает их в облако. При настройке устройства для Cloud Catalyst вся внутренняя дисковая память устройства выделяется под кэш MSDP. Одно устройство NetBackup 5240 CloudCatalyst поддерживает контейнер облачного хранилища емкостью до 1 петабайта.

Облако — отличный инструмент размещения резервных копий в отдельном хранилище. Однако нужно помнить о том, что при этом сохраняется возможность сетевого доступа к данным, и поэтому данный подход обеспечивает менее надежную защиту, чем магнитные ленты и AWS Glacier.

Дополнительные сведения о CloudCatalyst приведены в Руководстве по дедупликации Veritas NetBackup.

NetBackup AIR

Еще один способ создания резервных копий во внешнем хранилище заключается в применении технологии NetBackup Auto Image Replication (AIR). Резервные копии, созданные на одном устройстве NetBackup в одном домене NetBackup, можно реплицировать в одном или нескольких доменах NetBackup на других устройствах NetBackup.

Пользуясь NetBackup AIR, нужно понимать, что в разных доменах и на разных устройствах могут применяться разные конфигурации безопасности, что позволяет исключить доступ администратора одного домена NetBackup к резервным копиям, хранящимся в другом домене. Для применения AIR необходимо, чтобы у администратора был административный доступ как к исходной, так и к целевой системе.

Возможность реплицировать резервные копии в других доменах NetBackup, в том числе на других физических площадках, помогает реализовать несколько моделей аварийного восстановления.

- Модель один-к-одному: создание резервных копий из одного производственного ЦОД на одной площадке аварийного восстановления.
- Модель один-ко-многим: создание резервных копий из одного производственного ЦОД на нескольких площадках аварийного восстановления.
- Модель многие-к-одному: несколько удаленных офисов в разных доменах могут создавать резервные копии на устройстве в одном домене.
- Модель многие-ко-многим: удаленные центры обработки данных в нескольких доменах могут создавать резервные копии на нескольких площадках аварийного восстановления.

NetBackup поддерживает репликацию AIR из пула MSDP в одном домене NetBackup в пул MSDP в другом домене.

Дополнительные сведения приведены в Руководстве по дедупликации Veritas NetBackup.

ОБНАРУЖЕНИЕ: ВЫЯВЛЕНИЕ ВИРУСОВ-ВЫМОГАТЕЛЕЙ С ПОМОЩЬЮ ВСТРОЕННЫХ И ДОПОЛНИТЕЛЬНЫХ ИНСТРУМЕНТОВ

Первые признаки атаки вируса-вымогателя можно обнаружить слишком поздно: когда ничего не подозревающий пользователь попытается воспользоваться только что зашифрованными данными. Если факт шифрования данных не будет обнаружен достаточно быстро, зашифрованные данные могут оказаться в резервных копиях, что сделает восстановление этих копий бесполезным. Поэтому администраторы должны проявлять особую бдительность на стадии *обнаружения* вирусов-вымогателей. Упреждающий мониторинг помогает как можно раньше обнаружить атаку и приступить к ее нейтрализации, а также восстановлению зашифрованных и удаленных данных.

Для заблаговременного обнаружения вторжений и атак, позволяющего администраторам заранее нейтрализовать угрозу, можно пользоваться несколькими инструментами Veritas и других разработчиков. Примерами таких инструментов могут служить Veritas Information Map, NetBackup OpsCenter и Veritas Data Insight.

VERITAS INFORMATION MAP

Veritas Information Map — это мультиоблачное решение SaaS для управления данными, помогающее ИТ-специалистам оптимизировать нагрузку на хранилища данных, а также видеть более ясную картину своих структурированных и неструктурированных данных на единой сводной панели. Данное решение поддерживает разнообразные коннекторы Veritas для доступа к облачным, локальным и интегрированным хранилищам, что дает администраторам возможность собирать данные из всех своих систем.

В состав Information Map входят разнообразные *типы объектов*. Типы объектов характеризуют разные типы данных, которые Information Map может относить к тем или иным категориям для анализа. Один из типов объектов Information Map — *вирус-вымогатель*. Information Map сканирует данные через все поддерживаемые коннекторы и относит файлы к разным категориям исходя из расширений известных вирусов-вымогателей.

Информация, полученная с помощью типа объектов «вирус-вымогатель» Information Map, помогает администраторам выявлять, находить и изолировать файлы, отнесенные к категории вирусов-вымогателей. Вдобавок к этому появляется потенциальная возможность идентифицировать системы пользователя, вызвавшего атаку, по домашнему каталогу

или общей папке этого пользователя.

Дополнительные сведения о Information Map приведены на веб-сайте Information Map и в Руководстве по установке и администрированию Information Map.

NETBACKUP OPSCENTER

OpsCenter — это веб-приложение, помогающее организациям составить четкую картину состояния среды защиты данных NetBackup. С помощью OpsCenter администраторы могут следить за эффективностью резервного копирования, создавая комплексные отчеты. OpsCenter поставляется в двух версиях. Бесплатная версия называется OpsCenter, а расширенная платная версия — OpsCenter Analytics.

Данное приложение дает уникальную возможность пользователям NetBackup, применяющим пулы MSDP с резервным копированием. Метод шифрования, используемый в MSDP, отличается от распространенных методов шифрования вирусов-вымогателей. Шифрование MSDP не влияет на коэффициент дедупликации, потому что оно осуществляется после хэширования данных сегментов, а не до. Поэтому шифрование MSDP не влияет на коэффициент дедупликации так, как на него влияет шифрование вирусов-вымогателей.

Администраторы могут следить за коэффициентом дедупликации резервных копий с помощью OpsCenter. Внезапное резкое падение коэффициента дедупликации может указывать на то, что в резервную копию попадают только что зашифрованные файлы. В этой ситуации следует выяснить, что стало причиной данного изменения: обычные действия пользователей или вирус-вымогатель.

Еще один метод раннего обнаружения вредоносных действий заключается в мониторинге высокой интенсивности изменения данных. Этот метод подходит как для зашифрованных, так и для незашифрованных данных. Изменение 50 % или большего объема данных может указывать на то, что данные были зашифрованы. Помните о том, что уже зашифрованные данные могут шифроваться вновь и вновь.

Дополнительная информация о NetBackup OpsCenter приведена в Руководстве администратора Veritas NetBackup OpsCenter.

VERITAS DATA INSIGHT

Решение Data Insight предлагает средства анализа, слежения и подготовки отчетов, позволяющие обеспечить безопасность и учет использования файлов в организации. Разработанное для организаций с петабайтами данных и миллиардами файлов, решение Data Insight поддерживает интеграцию с решениями для архивации и системами безопасности, позволяющую предотвращать потерю данных и внедрять политики хранения информации.

- Автоматизация управления с помощью рабочих процессов и индивидуальной настройки.
- Повышение эффективности и экономичности сред хранения неструктурированных данных.
- Выполнение нормативных требований в отношении доступа к информации, ее использования и хранения.
- Защита конфиденциальной информации от несанкционированного доступа и раскрытия.

Программное обеспечение Veritas Data Insight поддерживает мониторинг доступа к файлам и автоматическую идентификацию пользователей данных по истории доступа. В состав продукта входят настраиваемые шаблоны отчетов, которыми можно пользоваться для обнаружения вирусов-вымогателей.

Data Insight сканирует неструктурированные системы и формирует историю доступа всех пользователей ко всем данным. Данное решение помогает организовать мониторинг и подготовку отчетности о доступе к конфиденциальной информации.

Veritas Data Insight периодически проводит аудит операций чтения, записи и переименования файлов в среде

хранения, находящейся под наблюдением. Отчеты о вирусах-вымогателях могут содержать информацию о количестве операций записи и переименования файлов, выполненных каждым пользователем. Превышение установленного порога может быть признаком того, что файлы, с которыми выполняются операции, стали объектом атаки.

Анализ внутренней угрозы

Veritas Data Insight — отличный инструмент, позволяющий администраторам определить, какие пользователи могут быть источником риска получения и раскрытия конфиденциальной информации, и принять меры к защите данных.

https://www.veritas.com/product/information-governance/data-insight/insider-threat

Дополнительные сведения о Veritas Data Insight приведены в Руководстве администратора Veritas Data Insight.

Подробная информация о шаблонах отчетов о вирусах-вымогателях приведена в следующих разделах:

Настраиваемые отчеты Data Insight

Шаблоны запросов DQL

ИНСТРУМЕНТЫ ДРУГИХ РАЗРАБОТЧИКОВ

Защита устройства резервного копирования — важная задача, но остальные компоненты пользовательских систем и производственные данные также должны быть в безопасности. Средства обнаружения вредоносных программ и вирусов-вымогателей, предлагаемые другими разработчиками, также могут пригодиться в обнаружении атак вирусов-шпионов на системы, отличные от устройств NetBackup, и защиты от таких атак. Дополнительные сведения об этих инструментах можно найти на веб-сайтах их разработчиков.

Symantec Endpoint Protection

Symantec Endpoint Protection обеспечивает обнаружение вредоносных программ и программ-шпионов, а также защиту физических и виртуальных серверов от вирусов. В состав продукта также входят средства обнаружения и предотвращения вторжений. См. веб-сайт Symantec Endpoint Protection.

Tripwire

Решение Trip применяется для мониторинга определенных видов изменений в файлах и поддерживает интеграцию с Symantec Endpoint Protection. См. Описание решения Tripwire/Symantec.

ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ: ПОСЛЕДНЯЯ СТАДИЯ ПОСЛЕ УСПЕШНОЙ АТАКИ ВИРУСА-ВЫМОГАТЕЛЯ

NETBACKUP

Гарантированной защиты от всех возможных угроз не существует. К сожалению, несмотря на все усилия на стадиях предотвращения и обнаружения атак, иногда атаки завершаются успехом, вынуждая организации ликвидировать их последствия. В зависимости от масштабов атаки, ее последствия могут представлять собой как несколько зашифрованных файлов на одном томе одной системы, так и тщательное уничтожение всех данных на целой площадке в несколько проходов. Независимо от масштабов целью атаки будут важнейшие данные компании. Ликвидация последствий атаки станет испытанием для инструментов и процедур аварийного восстановления.

В устройствах NetBackup Appliance полный набор продуктов NetBackup работает на аппаратном обеспечении, оптимизированном для высокой производительности. Эти устройства представляют собой защищенные комплексные решения для резервного копирования, хранения и дедупликации данных. Оптимизированная версия NetBackup, установленная на каждом устройстве NetBackup Appliance, помогает администраторам восстанавливать данные быстрее и эффективнее, чем прежде.

Устройства NetBackup Appliance дают администраторам резервного копирования возможность частичного и полного восстановления данных в случае их потери в результате вредоносных действий. Новые версии программного обеспечения содержат функции, помогающие дополнительно ускорить ликвидацию последствий атак.

Подробные инструкции по работе с решением NetBackup и устройствами NetBackup Appliance приведены в руководствах Руководство администратора Veritas NetBackup и Руководство администратора NetBackup Appliance.

NETBACKUP INSTANT ACCESS

Устройства NetBackup Appliance способны практически мгновенно создавать и восстанавливать резервные копии виртуальной машины целиком, не дожидаясь загрузки данных в виртуальную машину из резервной копии. NetBackup запускает виртуальную машину напрямую из резервной копии и мгновенно делает ее доступной пользователям целевого хоста ESX. Файлы (включая файлы vmdk) можно копировать без восстановления всей виртуальной машины. Для восстановления виртуальной машины нужно перенести файлы данных виртуальной машины из образа резервной копии на хост ESX с помощью VMware Storage vMotion.

Подробная информация об использовании данной возможности приведена в Руководстве администратора NetBackup for VMware.

NETBACKUP UNIVERSAL SHARE

Одна из новейших возможностей устройств NetBackup Appliance называется Universal Share. Она позволяет монтировать хранилища устройств NetBackup Appliance в качестве общих ресурсов NFS или CIFS и создавать резервные копии баз данных в средах, где отсутствуют агенты и API резервного копирования. Universal Share может применяться для хранения данных со сжатием и дедупликацией. Данный продукт также может быть очень полезен в качестве инструмента восстановления, поскольку он обеспечивает быстрый доступ к данным в резервных копиях.

NETBACKUP COPILOT FOR ORACLE INSTANT RECOVERY

Новая версия этого продукта создана на базе Oracle CoPilot и позволяет администраторам Oracle запускать базы данных непосредственно из хранилища устройства NetBackup Appliance.

Дополнительные сведения приведены в Руководстве администратора Veritas NetBackup™ for Oracle.

ПЕРЕДОВАЯ ПРАКТИКА

Выше уже обсуждались встроенные средства обеспечения безопасности, размещение резервных копий в других хранилищах и создание воздушных зазоров. Помимо этого, организациям рекомендуется принимать дополнительные меры по защите своей инфраструктуры резервного копирования от кибератак.

Очень важно защитить как данные в производственных системах, так и резервные копии данных в ЦОД. Именно инфраструктура резервного копирования и восстановления отвечает за восстановление работоспособности организации после крупномасштабной потери данных. Компании должны принимать все возможные меры для защиты резервных копий. Поверхностный подход к соблюдению рекомендаций и применению имеющихся мер защиты может стать крупнейшей уязвимостью организации. Хотя следующий список далеко не исчерпывающий, он содержит полезные рекомендации по дополнительным мерам предотвращения атак и минимизации их последствий.

- Вполне может быть, что выполнять процедуры аварийного восстановления придется не тем, на кого формально возложена эта ответственность. Процедуры аварийного восстановления всех важных данных организации должны быть полностью документированы и доступны — даже в чрезвычайных ситуациях. Кроме того, эти процедуры необходимо регулярно отрабатывать. Процедуры аварийного восстановления будут проходить проверку в реальном времени, когда их потребуется выполнить из-за настоящего происшествия или кибератаки. Самый неподходящий момент для того, чтобы узнать, что программное обеспечение, оборудование или процедуры резервного копирования не работают — это чрезвычайная ситуация, в которой потребуется ими воспользоваться. Лучше всего отрабатывать эти процедуры до возможной атаки, чтобы дать администраторам время устранить проблемы с неработающим оборудованием, программным обеспечением и процедурами. Также рекомендуется отрабатывать эти процедуры для успешного прохождения аудита безопасности. Процедуры резервного копирования и восстановления важных данных необходимо отрабатывать особенно часто. Внутренний вредитель с достаточными правами доступа может начать шифровать данные заблаговременно, чтобы зашифрованные данные со временем оказались во всех резервных копиях, а у компании в итоге не осталось ни одной полезной точки восстановления с незашифрованными данными.
- Администраторам резервного копирования должны быть известны последние точки восстановления и продолжительность восстановления всех типов данных. Резервные копии могут храниться на другой площадке, на магнитной ленте или в облаке, что потребует дополнительного времени на их восстановление. Администраторы резервного копирования должны знать, сколько времени нужно на восстановление, чтобы правильно информировать конечных пользователей.
- В операционных системах постоянно обнаруживают новые уязвимости, после чего разработчики выпускают исправления. Очень часто именно эти известные уязвимости операционных систем используются вредоносными программами и вирусами-вымогателями и дают им возможность распространяться на новые системы. У отдельных пользователей и в отдельных организациях могут быть установлены не все обновления операционных систем, и это приводит к появлению дыр в защите, позволяющих вредоносным программам распространяться. Своевременная установка обновлений крайне важна для минимизации последствий атаки.
- Права доступа должны быть максимально ограничены: необходимо предоставлять минимальный объем доступа, необходимый сотрудникам для выполнения своих обязанностей. Даже учетным записям администраторов необходимо предоставлять только минимальный объем полномочий, необходимый для выполнения их административных задач.
- Проводите проверку благонадежности администраторов, которые будут иметь доступ к данным компании и постоянно работать с ними. Чем шире доступ пользователя или администратора, тем более разрушительны потенциальные последствия его вредоносных действий. Внутренние вредители могут получить неограниченный доступ к служебной информации после того, как они окажутся в компании, и проверка благонадежности — один из способов защиты от подобных угроз.
- Регулярно меняйте пароли всех встроенных учетных записей, включая пароли устройств NetBackup. В частности, это относится к учетным записям admin и maintenance хоста, а также sysadmin и nbasecadmin RMM.
- Знакомьтесь с техническими уведомлениями Veritas, которые публикуются на веб-сайте службы поддержки Veritas по адресу https://www.veritas.com/content/support/en_US.html

- Принимайте дополнительные меры по защите важнейших метаданных NetBackup:
    - Адаптируйте стандартную политику резервного копирования главного каталога.
    - Настройте политику резервного копирования для сервера управления ключами NetBackup (KMS).

РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ УСТРОЙСТВ

Veritas предлагает подробное руководство по безопасности, в котором приведена информация о средствах защиты, входящих в состав всех устройств NetBackup Appliance с программным обеспечением версии 3.1 или выше. Рекомендуется перечитывать это руководство при развертывании устройств NetBackup Appliance. По умолчанию на устройствах NetBackup Appliance включены общие средства безопасности, а настройка расширенных инструментов оставлена на усмотрение пользователей. Для обеспечения максимальной безопасности необходимо настроить и применять все средства защиты.

В их число входят:

- Аутентификация и авторизация пользователей
- Предотвращение и обнаружение вторжений
- Средства обеспечения безопасности операционной системы
- Средства обеспечения целостности и безопасности данных
- Веб-интерфейс, сеть, система автоматического обращения за помощью и средства безопасности IPMI
- Брандмауэр

Настоятельно рекомендуется перечитывать данное руководство и настроить все средства безопасности на каждом устройстве NetBackup Appliance. Рекомендуем ознакомиться с электронным Руководством по безопасности устройств Veritas NetBackup™ Appliance.

ЗАКЛЮЧЕНИЕ

Вирусы-вымогатели и внутренние вредители представляют собой серьезную угрозу, и вдобавок к этому постоянно выявляются новые уязвимости операционных систем. Часто появляются новые варианты известных вредоносных программ и вирусов-вымогателей. Всегда существует угроза перехода по неправильной ссылке или открытия сообщения электронной почты с вирусом. Несмотря на все усилия администраторов по защите данных, вирусам-вымогателям и внутренним вредителям иногда удается добраться до важнейших данных организации.

Программное обеспечение Veritas NetBackup считается эталоном в сфере аварийного восстановления на протяжении нескольких десятилетий. В состав каждого устройства NetBackup Appliance входят адаптированная операционная система Linux, оптимизированная версия NetBackup и встроенная версия Symantec Data Center Security.

В связке с локальными и облачными хранилищами данных устройства NetBackup Appliance обеспечивают отличную защиту от вирусов-вымогателей и внутренних вредителей. Устройства NetBackup Appliance помогают администраторам резервного копирования уменьшить риски и ускорить ликвидацию последствий атак любого масштаба.

СПРАВОЧНАЯ ИНФОРМАЦИЯ

- Национальный центр компетенции по кибербезопасности (NCCoE), входящий в состав Национального института стандартов и технологий США (NIST), подготовил специальную публикацию под названием *Data Integrity: Recovering from Ransomware and Other Destructive Events (Целостность данных: ликвидация последствий атак вирусов-вымогателей и других деструктивных событий)*. Этот обширный документ состоит из трех частей и содержит подробное описание стратегий защиты от вредоносных действий и мер по ликвидации последствий кибератак.

  Специальная публикация NIST 1800-11

  Data Integrity: Recovering from Ransomware and other Destructive Events (главная страница)

  - NIST SP 1800-11a: Резюме
  - NIST SP 1800-11b: Подход, архитектура и характеристики защиты: что мы разработали и почему
  - NIST SP 1800-11c: Практические руководства: инструкции по созданию эталонного решения
- Руководство по безопасности устройств Veritas NetBackup Appliance: https://www.veritas.com/support/en_US/doc/96220900-132543872-0/
- Компьютерная команда экстренной готовности США: варианты резервного копирования данных: https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf
- Руководство администратора Veritas NetBackup в облаке: https://www.veritas.com/support/en_US/doc/58500769-132715871-0/
- Руководство по дедупликации Veritas NetBackup: https://www.veritas.com/support/en_US/doc/25074086-131900563-0/
- Руководство по применению устройств Veritas NetBackup Appliance в сетях Fibre Channel: https://www.veritas.com/support/en_US/doc/99943943-132539628-0/
- Веб-сайт Veritas Information Map: https://www.veritas.com/informationmap/
- Руководство по установке и администрированию Veritas Information Map: https://www.veritas.com/support/en_US/doc/109835244-109835565-0/
- Видео на YouTube: поиск вирусов-вымогателей с помощью Veritas Information Map: https://youtu.be/xOkWUCH9plg
- Руководство администратора Veritas NetBackup OpsCenter: https://www.veritas.com/support/en_US/doc/27537447-133302844-0/
- Руководство администратора Veritas Data Insight: https://www.veritas.com/support/en_US/doc/133377453-133377456-0/
- Руководство пользователя Veritas Data Insight: https://www.veritas.com/support/en_US/doc/133376979-133376982-0/
- Анализ внутренней угрозы: обнаружение и защита с помощью Veritas Data Insight: https://www.veritas.com/product/information-governance/data-insight/insider-threat

Подробная информация о шаблонах отчетов о вирусах-вымогателях приведена в следующих разделах Руководства пользователя:

  - Настраиваемые отчеты Data Insight

    https://www.veritas.com/content/support/en_US/doc/133376979-133376982-0/DI_6_1_2_v109979856-133376982

  - Шаблоны запросов DQL

    https://www.veritas.com/content/support/en_US/doc/133376979-133376982-0/DI_6_1_2_v109979871-133376982

- Веб-сайт Symantec Endpoint Protection: https://www.symantec.com/products/endpoint-protection
- Описание решения Tripwire/Symantec: https://www.symantec.com/content/dam/symantec/docs/partners/solution-brief/technology-partner-tripwire-en.pdf
- Руководство администратора устройства Veritas NetBackup: https://www.veritas.com/support/en_US/doc/75895731-133007275-0/
- Руководство администратора Veritas NetBackup, том I: https://www.veritas.com/support/en_US/doc/18716246-132504715-0/
- Руководство администратора Veritas NetBackup для VMware: https://www.veritas.com/support/en_US/doc/21902280-133434834-0/
- Руководство администратора Veritas NetBackup для Oracle: https://www.veritas.com/support/en_US/doc/16226115-133434979-0/
- Нерассказанная история о NotPetya — самой разрушительной кибератаке в истории: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- Городской совет Атланты тратит 2,6 миллиона долларов на ликвидацию последствий атаки вируса-вымогателя, требовавшего 52 000 $: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/
- Шотландский пивоваренный завод ликвидирует последствия атаки вируса-вымогателя: https://www.theregister.co.uk/2018/09/21/arran_brewery_ransomware/
- Услуги по ведению переговоров с киберпреступниками, вымогающими биткойны: https://bitcoinist.com/negotiating-bitcoin-ransomware-with-cyber-criminals/

ЮРИДИЧЕСКИЕ ЗАЯВЛЕНИЯ

НАСТОЯЩАЯ ПУБЛИКАЦИЯ ПРЕДОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ», БЕЗ КАКИХ БЫ ТО НИ БЫЛО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ УСЛОВИЙ, ЗАЯВЛЕНИЙ И ГАРАНТИЙ, В ТОМ ЧИСЛЕ БЕЗ КАКИХ БЫ ТО НИ БЫЛО ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ ТОВАРНОЙ ПРИГОДНОСТИ, ПРИМЕНИМОСТИ В КАКИХ БЫ ТО НИ БЫЛО ЦЕЛЯХ И НЕНАРУШЕНИЯ ПРАВ ТРЕТЬИХ ЛИЦ, ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЕВ, КОГДА ОТКАЗ ОТ ПРЕДОСТАВЛЕНИЯ ТАКИХ ГАРАНТИЙ НЕ ИМЕЕТ ЮРИДИЧЕСКОЙ СИЛЫ. КОМПАНИЯ VERITAS TECHNOLOGIES LLC НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ПОБОЧНЫЙ И КОСВЕННЫЙ УЩЕРБ, ВЫЗВАННЫЙ ПРЕДОСТАВЛЕНИЕМ, СОДЕРЖАНИЕМ И ПРИМЕНЕНИЕМ НАСТОЯЩЕЙ ПУБЛИКАЦИИ. СОДЕРЖАНИЕ ДАННОГО ДОКУМЕНТА МОЖЕТ БЫТЬ ИЗМЕНЕНО БЕЗ УВЕДОМЛЕНИЯ.

О КОМПАНИИ VERITAS TECHNOLOGIES LLC

С помощью Veritas Technologies организации любого размера получают максимальную отдачу от их основного актива — информации. Платформа Veritas позволяет ускорить цифровую трансформацию и упростить решение таких задач, как управление информацией в мультиоблачных средах, защита данных и оптимизация хранения, соблюдение нормативных требований и переносимость между облачными вендорами. Восемьдесят шесть процентов компаний из списка Fortune 500 используют решения Veritas для получения конкурентных преимуществ за счет интеллектуальной работы с данными. Узнайте больше на http://www.veritas.com/ или подпишитесь на нас в Twitter: @veritastechllc.

ООО «Веритас Текнолоджис»
БЦ «Смоленский Пассаж»,
Смоленская пл., д. 3, 10 этаж,
121099, Москва, Россия
Телефон: +7 (499) 955-2960
www.veritas.com

Адреса и контактные номера телефонов представительств в разных странах можно узнать на нашем веб-сайте.

https://www.veritas.com/about/contact.html

VERITAS

Истина в информации.