Обзор решения

Как модель Information Centric Security решает проблему GDPR

Введение

В Генеральном регламенте Европейского союза о защите персональных данных (General Data Protection Regulation, GDPR) основное внимание уделяется безопасности данных и конфиденциальности. Действие этого регламента распространяется и за пределы ЕС: его обязаны соблюдать все организации, которые хранят или обрабатывают персональные данные физических лиц («субъектов персональных данных») на территории ЕС. Регламент вступит в силу 25 мая 2018 года, но он уже оказывает существенное влияние на подходы к разработке, внедрению и обслуживанию систем информационной безопасности.

В основе GDPR лежит концепция, относящая право на конфиденциальность к числу базовых прав человека. Согласно этому регламенту, организации обязаны учитывать требования к конфиденциальности данных и, как следствие, к их безопасности, уже на этапе проектирования. Компания Symantec считает, что в фокусе информационной безопасности должны находиться не устройства, сети или пользователи, а данные. Такой подход решает сразу множество проблем, стоящих сегодня перед организациями, и в том числе помогает соблюсти многие требования GDPR.

Вы готовы?

GDPR вступает в силу в мае 2018 года, однако многие организации все еще находятся на этапе разработки планов и не готовы к новому регламенту. По данным исследования, проведенного компанией Symantec в октябре 2016 года, 90 % организаций считают регламент GDPR проблемой, требующей решения, но только 26 % уверены, что смогут полностью выполнить его требования. Защита данных — важная задача, которую нужно правильно решать с самого начала.

Последствия несоблюдения требований

Неспособность должным образом защитить информацию не только подрывает доверие к организации, но зачастую парализует ее работу, наносит ущерб бренду и приводит к финансовым потерям. Кроме того, регулирующие органы наделены правом подвергать организации весьма существенным штрафам — до 20 млн евро или 4 % годового оборота (в зависимости от того, что больше).

В случае нарушения порядка доступа к данным организации обязаны уведомить регулирующие органы и всех затронутых пользователей в течение 72 часов. Без качественных политик в отношении конфиденциальных данных (включая управление рисками, контроль за использованием и размещением данных, контроль нарушений и планы реагирования) исполнить это требование весьма затруднительно. Однако задача существенно упрощается, если организация способна продемонстрировать, что данные надежно защищены (например, с помощью шифрования).

Что считается персональными данными?

Персональные данные определены следующим образом: «любая информация, относящаяся к физическому лицу, в том числе к его частной, профессиональной или общественной жизни. Это может быть имя, фотография, адрес электронной почты, банковские реквизиты, медицинская информация, сообщения в социальных сетях или IP-адрес компьютера».

Основные положения GDPR

GDPR – всеобъемлющий документ, который содержит множество положений, касающихся не только технологий, но и политик, систем и поведения сотрудников организации. Тем не менее, поскольку основной целью GDPR является защита конфиденциальных данных, некоторые ключевые принципы найдут свое отражение в любой стратегии безопасности, фокусирующейся на защите данных на всем их жизненном цикле.

Требования:

ПОДГОТОВКА

ЗАЩИТА

ВЫЯВЛЕНИЕ

РЕАГИРОВАНИЕ

Идентифицируйте персональные данные: определите, какие персональные данные вы собираете и как они хранятся.

Оцените систему защиты данных: определите, обеспечивают ли имеющиеся политики и процедуры достаточный уровень защиты данных от утечки и несанкционированного доступа.

Учтите конфиденциальность: учтите во всех технологиях и процессах требования конфиденциальности и разработайте процессы защиты персональных данных.

Защитите персональные данные: внедрите полноценное управление рисками, связанными с персональными данными. Контролируйте, кто имеет доступ к данным, где они расположены, как используются и защищены ли они с помощью надежных технологий.

Контролируйте перемещение персональных данных: перемещение персональных данных за пределы ЕС (например, в облако) подлежит тщательному надзору со стороны регулятора.

Проверьте процессы реагирования на нарушения: убедитесь, что в вашей компании есть инструменты, позволяющие за 72 часа определить масштабы нарушения.

Information Centric Security

В основе концепции Information Centric Security лежит принцип ориентированности на защиту данных. Уникальное сочетание технологий защиты данных и аналитики позволяет организациям идентифицировать, отслеживать и защищать конфиденциальную информацию, включая данные, которые переносятся в облако или используются сторонними организациями. Для борьбы с нарушениями порядка доступа к данным применяются инструменты аналитики, позволяющие выявлять подозрительных пользователей и удаленно ограничивать их доступ к документам — обеспечивая тем самым защиту от утечки данных в реальном времени.

Как Information Centric Security помогает выполнить требования GDPR

Для многих организаций принятие GDPR послужило поводом для пересмотра и улучшения принципов защиты персональных данных. Мы предлагаем начать с поиска ответов на следующие основополагающие вопросы:

1. **Каким основным рискам подвергается имеющаяся система защиты данных?**
2. **Как идентифицировать и отслеживать конфиденциальные данные, где бы они ни находились?**
3. **Как защитить данные и гарантировать, что доступ к ним имеют только авторизованные пользователи?**
4. **Если нарушение все же произойдет, как на него реагировать?**

В этом разделе мы подробно расскажем, как технологии Symantec Information Centric Security помогут вам ответить на заданные вопросы.

1 Каким рискам подвергается система защиты данных?

Компания Symantec помогает определить степень защиты конфиденциальных данных и оценить сопутствующие риски. Процесс предотвращения утечки данных (DLP), предлагаемый компанией Symantec, позволяет превентивно вычислять угрозы еще до того, как они превратились бы в реальную проблему.

Этот процесс состоит из пассивного мониторинга DLP и «сканирования» корпоративной сети в поисках уязвимых бизнес-процессов и потенциальной вредоносной деятельности. Результатом является информация о том, где хранятся конфиденциальные данные, куда они передаются и как сотрудники работают с ними. Обобщенные данные результатов сканирования DLP свидетельствуют о том, что каждый пятидесятый файл в корпоративной сети доступен слишком большому числу пользователей, а каждое четырехсотое сообщение электронной почты содержит конфиденциальную информацию, которая может быть передана без защиты.

Задачей оценки киберугроз занимается служба Symantec Information Centric Analytics (ICA) от Bay Dynamics. Эта служба анализирует огромные объемы информации, поступающей от систем защиты данных, и вычисляет подозрительных пользователей и подозрительные действия. Полученные результаты помогают вырабатывать новые стратегии защиты данных и уточнять имеющиеся политики. Для оценки рисков могут применяться исторические и актуальные сведения о поведении и инцидентах с данными. Подобный поведенческий анализ пользователей и сущностей помогает выявлять инсайдерские риски, способные привести к утечке данных.

2 Как идентифицировать конфиденциальные данные?

Для того чтобы защитить конфиденциальные данные (включая те из них, что упомянуты в GDPR), необходимо сначала найти их в сети организации — на общих дисках, в базах данных и на конечных устройствах — и

Рекомендации:

- Разумно используйте оставшееся время, поскольку внедрение может занять дольше запланированного.
- Заручитесь поддержкой совета директоров, информируйте его о ходе реализации программы.
- Идентифицируйте и оцените риски, связанные с конфиденциальностью и безопасностью больших данных.
- Составьте перечень используемых персональных данных и обеспечьте законное обращение с ними.
- Определите круг задач, которые можно решить с помощью технологий:
  - **Подготовка:** описание информационной среды (и используемых данных), определение рисков.
  - **Защита:** всесторонняя защита персональных данных.
  - **Выявление:** мониторинг и выявление нарушений.
  - **Реагирование:** составление плана реагирования на инциденты.

провести инвентаризацию. В состав Symantec Data Loss Prevention входят стандартные и настраиваемые политики GDPR, позволяющие автоматически находить данные определенных типов в соответствии с Регламентом, защищать их и применять подходящие методы реагирования на инциденты. DLP отслеживает данные, где бы они ни находились и куда бы они ни передавались — как по сетевым протоколам (например, по электронной почте или через веб), так и напрямую с конечных устройств (например, через съемные носители или буфер обмена).

Пользователям, создающим конфиденциальные данные, Symantec дает удобные инструменты их классификации и применения визуальных меток, информирующих других сотрудников о конфиденциальном характере данных.

Благодаря интеграции Symantec DLP с CloudSOC (брокером безопасного доступа к облачным ресурсам) структурированные или неструктурированные конфиденциальные данные также могут идентифицироваться и отслеживаться в облачных сервисах.

Применение DLP снижает вероятность утечки данных за счет применения автоматизированных процессов уведомления конечных пользователей о действиях, которые подвергают риску персональные данные.

Заметным источником нарушений являются внутренние злоумышленники и несанкционированные пользователи, получившие доступ к данным. Продукт Symantec Information Centric Analytics соотносит информацию о правах доступа пользователей с данными о фактическом обращении к конфиденциальной информации и позволяет своевременно узнавать об обычном и, что еще важнее, необычном поведении пользователей.

3 Как защитить данные и контролировать права доступа?

Решение Symantec Information Centric Security (ICS) обеспечивает полную безопасность персональных данных на всем их жизненном цикле за счет контроля доступа и выборочного шифрования, определяемого политиками. Компонент предотвращения утечки данных, брокер безопасного доступа к облачным ресурсам и функция классификации данных выявляют конфиденциальную информацию, а компонент Information Centric Encryption (ICE) зашифровывает ее для безопасной передачи. Symantec Information Centric Encryption обеспечивает автоматическую защиту конфиденциальной информации при ее отправке за пределы компании — поставщикам, партнерам, подрядчикам и дочерним компаниям. В целях разделения обязанностей с облачными сервисами и внешними службами безопасности ключи шифрования всегда остаются в руках организации.

Благодаря двухфакторной аутентификации (2FA) Symantec VIP доступ к данным получают только авторизованные пользователи — из любого места и с любого устройства. Возможности DLP также позволяют контролировать передачу данных получателям, не обладающим доверием, и сторонним организациям, которые не соблюдают регламент GDPR. Ограничение доступа к данным в облаке по географическому признаку обеспечивается шлюзом CASB. В случаях, когда требуется уничтожение цифровой информации, доступ к данным может быть централизованно отозван в любой момент.

4 Как обнаружить нарушение и отреагировать за 72 часа?

Выявление нарушений — непростая задача, и зачастую организации узнают об утечке только через долгое время после инцидента.

Индикаторы компрометации могут быть получены из множества источников, однако анализ этой обширной и разнородной информации является весьма ресурсоемким. Обширная информация о защите данных, предоставляемая решением Symantec Information Centric Security, анализируется службой Symantec Information Centric Analytics вместе со сведениями о доступе к данным (телеметрией учетных данных), информацией о корпоративных ресурсах и предупреждениями из других систем безопасности (телеметрией угроз). Information Centric Analytics помогает выявлять аномалии в поведении отдельных пользователей или компьютеров, свидетельствующие о возможных злонамеренных

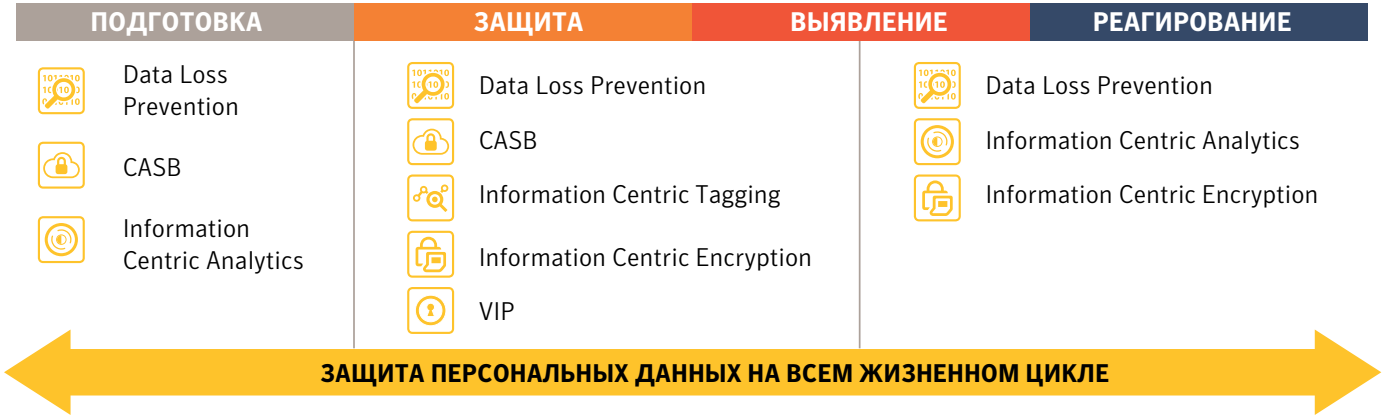
Дополнительные решения Symantec:

- **Symantec Control Compliance Suite** — помогает идентифицировать и анализировать риски с помощью функции GDPR Readiness Assessment, а также предоставляет механизм контроля за соблюдением политик.
- **Secure Web Gateway** — используется совместно с DLP для предотвращения утечки конфиденциальной информации через несанкционированные облачные приложения (через так называемые «теневые ИТ»).
- **Symantec Complete Endpoint Security** — позволяет реализовать комплексную стратегию предотвращения и обнаружения несанкционированного доступа к данным на корпоративных конечных точках.
- **Symantec Cloud Workload Protection** — обеспечивает безопасность при работе с облачными сервисами: ЦОД, публичными и частными облаками.
- **Symantec Data Center Security** — обеспечивает полную защиту серверов и микросегментацию рабочих процессов в ЦОД и частных облаках.
- **Symantec Email Security** — обеспечивает безопасность электронной почты с помощью передовых технологий защиты от спама и угроз.
- **Symantec Endpoint Encryption** — защищает конфиденциальную информацию путем надежного шифрования всего жесткого диска и съемных носителей.
- **Symantec Cloud Data Protection** — обеспечивает шифрование и маркировку конфиденциальных данных в приложениях SaaS с целью соблюдения рекомендаций GDPR по псевдонимизации.
- **Cyber Security Services** — оптимизирует систему кибербезопасности, используя опыт Symantec и анализ угроз для нейтрализации каждого этапа атаки.
- **Education Services** — помогает углубить ваши знания продуктов и проверить технические навыки, чтобы использовать инвестиции в ИТ с максимальной отдачей.
- **Consultancy Services** — оказывает поддержку при разработке, оптимизации и внедрении системы безопасности, чтобы обеспечить надежную защиту и использовать инвестиции с наибольшей пользой.

действиях сотрудника или о захвате учетной записи. Функции прослеживания позволяют сопоставить пользователей с инцидентами DLP и выяснить, какие конфиденциальные данные были раскрыты и почему. Компания Symantec также предлагает решения для мониторинга угроз, такие как Advanced Threat Protection и Cyber Security Services.

Для демонстрации того, что данные были надежно защищены, могут применяться отчеты о шифровании. Благодаря централизованному мониторингу доступа к данным организации могут отслеживать, кто и откуда обращался к конфиденциальной информации после нарушения. Даже если данные были раскрыты авторизованными пользователями, их доступ может быть оперативно отозван.

Обеспечение конфиденциальности и безопасности данных с помощью Symantec Information Centric Security



Краткие выводы

Information Centric Security помогает обеспечить соблюдение Генерального регламента о защите персональных данных (GDPR) путем формирования комплексной стратегии защиты информации. Для этого применяются заранее настроенные политики GDPR, прослеживаемые процедуры защиты конфиденциальной информации в управляемых и неуправляемых средах, а также анализ инцидентов, связанных с нарушением порядка доступа к данным.

О компании Symantec

Symantec Corporation (NASDAQ: SYMC) — лидирующая компания в сфере кибербезопасности. Мы обеспечиваем защиту важных данных как частных пользователей, так и крупных компаний, включая государственные учреждения. Интегрированные решения Symantec используются организациями в разных странах для защиты от комплексных атак на конечные точки, облачные среды и инфраструктуру. Более 50 миллионов индивидуальных пользователей и семей во всем мире доверяют продуктам Norton и LifeLock защиту своих домашних и личных устройств. Под управлением компании Symantec находится одна из крупнейших гражданских сетей анализа киберугроз, что позволят нам распознавать и блокировать самые изощренные угрозы. Дополнительные сведения см. на веб-сайте www.symantec.com или на наших страницах в Facebook, Twitter и LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 США | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_SB_InfoCentricSecurity_GDPR_EN_v1a