perimetrix

Data Leakage Prevention DLP Data Leakage Prevention DLP Data Leakage Prevention DLP Data Leakage Prevention DLP Data Leak-
DLP Data Leakage Prevention DLP Data Leakage
Data Leakage Prevention DLP Data Leakage Pre-
kage Prevention DLP Data Leakage Preven-
DLP Data Leakage Prevention

КЛАССИФИКАЦИЯ И ЗАЩИТА БИЗНЕС СВЕДЕНИЙ

Data Leakage Prevention DLP Data Leak-
Data Leakage Prevention DLP Data Leakage
Data Leakage Prevention DLP Data Leakage Pre

ПОЧЕМУ DLP НИЧЕГО НЕ “ПРЕДОТВРАЩАЕТ” И ЧТО НА САМОМ ДЕЛЕ НЕОБХОДИМО

ВОПРОС: Ключевая задача DLP-системы[1]—предотвращение утечки техническими методами. Какие способы обхода DLP-систем могут использовать инсайдеры и как им противостоять?

От самого простого способа — архива с паролем — до построения SSL–туннелей и использования клиента TOR. Противостоять нужно путем применения четких и жестких политик безопасности и специализированных решений, основанных на применении *Data–Centric Security*. При таком подходе фокус защитных мероприятий переносится от контроля над каналами к контролю над данными, что позволяет:

— идентифицировать и защитить все информационные активы независимо от их расположения как внутри периметра организации, так и вне его;

— ограничить и строго контролировать доступ к данным конфиденциального характера через все сети, устройства, информационные системы, сервисы и прочее;

— протоколировать и инспектировать все действия, совершаемые с чувствительными данными;

— ускорить бизнес–процессы компании за счет использования защищенной цифровой экосистемы, включающей внутренних и внешних бизнес–пользователей и передовые технологии безопасности данных на протяжении их жизненного цикла.

ВОПРОС: Какие новые возможности открывает Perimetrix в части предотвращении утечки чувствительных данных?

Хотя наше решение тоже применяется для решения задач предотвращения утечки данных, нас нельзя относить к разработчикам DLP в его классическом понимании. Да, в нашей системе есть модуль, предназначенный для контроля некоторых каналов и протоколов передачи, по которым ценные данные могут «утечь» за пределы компании. Но мы считаем подход Perimeter–Based Security устаревшим, и в основе нашего решения лежит идея *Data–Centric Security*. Программный комплекс Perimetrix SafeSpace скорее можно отнести к классу EDRM–решений[2].

Основные ограничения DLP–систем связаны с невозможностью отслеживания всех каналов утечки и обработки всех форматов данных. Самое сложное при внедрении DLP–это определение данных, которые необходимо защищать, и всех возможных каналов утечки. Кроме того, необходимо ограничивать использование программ/протоколов/типов данных, которые не обрабатываются DLP–решением.

Если же требуется передать конфиденциальные данные «за периметр» организации, например партнерам, то как отследить, что они не «утекут» от партнера? Тут и возникает необходимость в IRM/EDRM–решениях[2]. IRM (Information Rights Management) позволяет удаленно контролировать использование данных. За счет шифрования файлов удается предотвратить неавторизованный доступ, а с помощью клиентских приложений удается ограничить возможные действия над документами. Но использование IRM ограничивается поддержкой на уровне пользовательских приложений.

Системы EDRM (Enterprise Digital Rights Management) позволяют контролировать доступ к данным: все документы шифруются, при этом ключи для расшифровки находятся на сервере и для получения доступа к ключам/серверу необходимо пройти аутентификацию. Что касается клиентских приложений (MS Word, Adobe Acrobat Reader и т.д.), то они работают под управлением агента EDRM, который гарантирует права использования документов. Классическим примером необходимости использования EDRM является защита конструкторской документации.

Допустим, к таким данным имеет доступ ограниченное число пользователей–конструкторов. Риск утечки может возникнуть в связи с тем, что нет средств контроля действий пользователей, которым разрешен доступ к такой информации. Ситуация: в связи с производственной необходимостью сотрудник конструкторского бюро копирует конфиденциальные данные на свой рабочий компьютер, а затем пересылает по электронной почте коллеге. Это вполне допустимо

1 **DLP** — Data Leak Prevention.

2 **IRM** — Information Rights Management; **EDRM** — Enterprise Digital Rights Management.

и является частью соответствующего бизнес–процесса. Однако в результате таких действий данные могут попасть к тем пользователям, которые не имеют соответствующих полномочий, или даже к злоумышленникам. Благодаря использованию EDRM неавторизованные пользователи не смогут получить доступ к защищаемой информации, при этом все попытки доступа протоколируются.

Контроль над движением информации конфиденциального характера осуществляется и в том случае, если данные находятся «за периметром», а доступ к ним может быть централизованно отменен в любой момент. Таким образом, совместное использование технологий DLP и EDRM очень и очень оправданно. DLP — хорошее решение для мониторинга коммуникаций, опознавания содержимого конфиденциального характера с последующим оповещением или блокировкой передачи данных. EDRM — для обеспечения безопасного документооборота, в который вовлечено ограниченное число ответственных сотрудников организации и, возможно, внешних контрагентов.

ВОПРОС: Чего ждать от разработчиков DLP-систем в обозримом будущем и куда движется отрасль?

С учетом сегодняшнего ландшафта угроз информационной безопасности очевидно, что требуется совместное применение технологий DLP и EDRM в рамках подхода *Data–Centric Security*. Первые интегрированные решения нового класса (IRM/EDRM + DLP) создавались из продуктов разных разработчиков, поэтому большого развития и популярности они не получили.

Сегодня мировые вендоры идут по пути, когда одна компания приобретает другую с целью интеграции в единый продукт. Последний пример такого явления — приобретение Symantec португальской компании Watchful Software с целью создания Symantec Information Centric Tagging и последующей реализации подхода Data–Centric Security из следующего набора решений:

— Symantec Information Centric Tagging.
— Symantec Data Loss Prevention.
— Symantec Information Centric Encryption.
— Symantec Validation and ID Protection Service.

Далее, на наш взгляд, вендоры задумаются об интеграции DLP/EDRM, контроля привилегированных пользователей PIM[3] и решений класса IDM[3] в один продукт. Такой подход позволит эффективнее решать следующие задачи службы безопасности:

— защита от утечек конфиденциальной информации;
— борьба с вредительством;
— борьба с проявлениями саботажа;
— соответствие требованиям регуляторов;
— усиление традиционных мер защиты информации.

ВОПРОС: В чем суть реализации вашего подхода на практике?

ОВ основе нашего подхода к защите ценных данных лежит методология DCSM (*Data Centric Security Model*), или информационно–центричная модель безопасности, основной фокус которой нацелен на обеспечение данных соответствующим уровнем безопасности в зависимости от их бизнес–ценности. Существует несколько классификаций бизнес–информации в зависимости от ее ценности и вовлеченности в бизнес–процесс, где она обрабатывается. Такая классификация позволяет динамически управлять полномочиями как пользователей, так и приложений (процессов).

Внедрение подхода DCSM начинается с формирования набора руководящих принципов корпоративной обработки данных, которые, в свою очередь, определяют политики безопасности и сервисы ИБ, необходимые для поддержки этих руководящих принципов.

После идентификации информационных активов и классификации данных становится возможным определение бизнес–ориентированных правил управления этими данными для каждой категории информации. Допустимые действия

3 **PIM** — Personal Infromation Management; **IDM** — Identity Data Management.

с классифицированными данными суммируются в политики, определяющие все аспекты использования защищаемых данных в процессах их создания, обработки, хранения и передачи, на всем протяжении их жизненного цикла, от создания до утраты полезности. Эти политики транслируются в настройки ИБ–сервисов и прикладные пользовательские системы, образуя прочную связь между бизнесом и ИТ–технологиями, которые теперь могут быть сфокусированно применены в необходимом контексте.

Реализуя ядро концепции DCSM, наш программный комплекс Perimetrix SafeSpace (PSS) обеспечивает классификацию ценных данных и соблюдение устанавливаемых правил работы с данными, динамически контролируя и ограничивая отступления от этих правил. Любые действия пользователей и процессов, так или иначе не укладывающиеся в рамки разрешений, блокируются, и, таким образом, защищаемые данные могут существовать и использоваться только в пределах четко определенного периметра.

Каждый проект внедрения PSS предполагает не только развертывание самого ПО, но и существенную часть работ, направленных на обследование бизнес–процессов, в рамках которых ведется обработка ценной информации в электронном виде и последующее построение модели ее защиты. Реализация режима конфиденциальности в отношении информации в электронной форме должна основываться на методологии управления рисками, учитывающей бизнес–требования, что предполагает приоритетное обеспечение конфиденциальности данных в тех рабочих процессах, где ее нарушение может нанести наибольший ущерб компании. Как правило, такими рабочими процессами являются конфиденциальный документооборот, внутрикорпоративная переписка по электронной почте, обработка данных в системе управления персоналом, финансовых и конструкторских данных разрабатываемых приборов и изделий, ноу–хау, схемы и методики производственных технологических процессов и т.д.

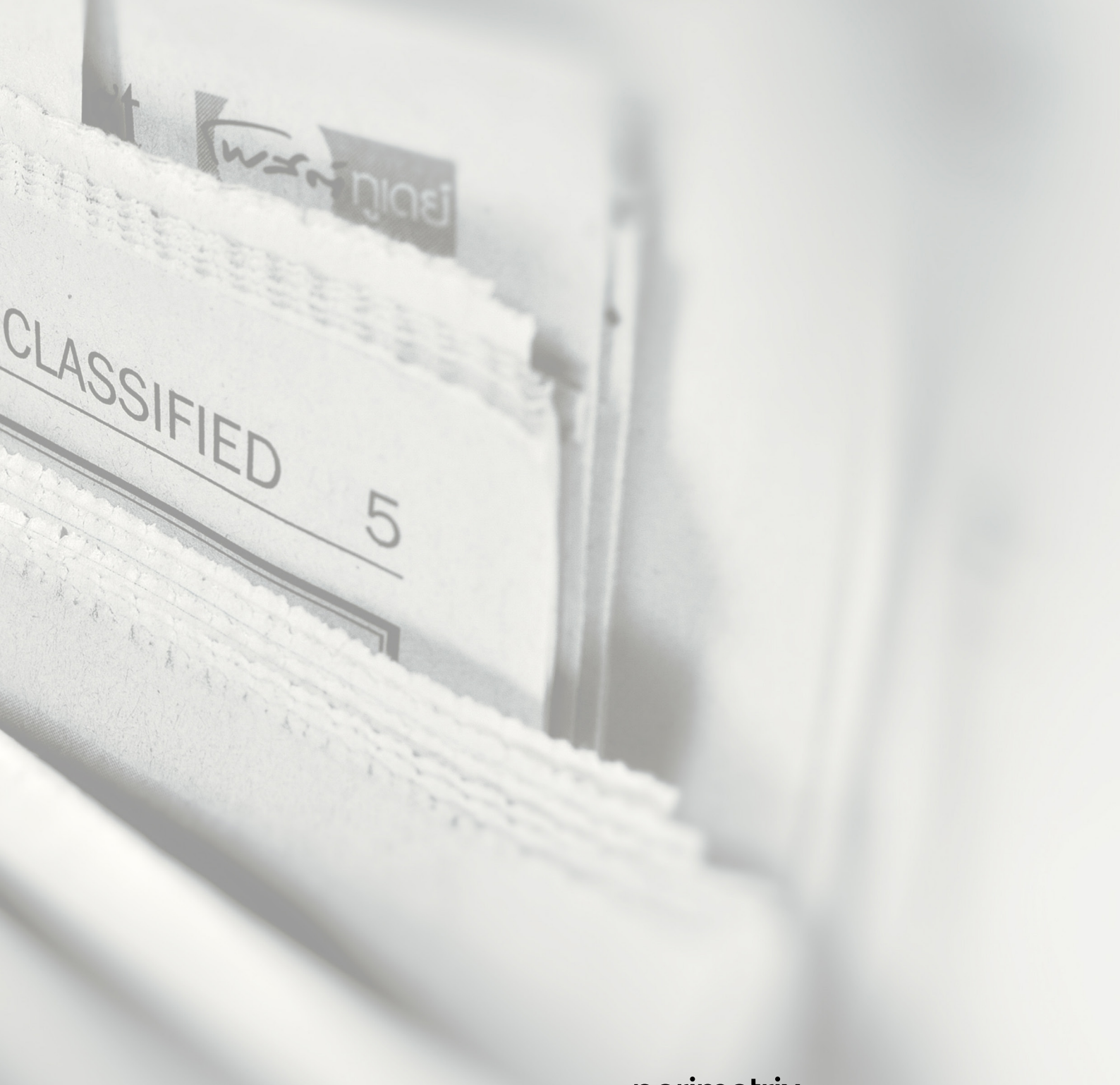
Порядок анализа рабочих процессов нами проработан достаточно подробно. Мы не только выделяем подпроцессы, происходящие непосредственно в электронной среде, но и принимаем во внимание требуемые ограничения по работе с конфиденциальной информацией до и после ее преобразования в электронный вид. Результатом консалтинговой части проекта является детальная модель защиты информации, в которой описывается планируемая классификация защищаемых электронных данных и порядок нанесения на них неотрывных классификационных меток, допустимые места и форматы хранения защищаемых данных, допустимые приложения для обработки, каналы их передачи и правила преобразования из электронной формы в иные физические. Кроме того, в модели защиты определяются полномочия пользователей по работе с электронными конфиденциальными данными в тех или иных рабочих процессах.

Модель защиты затем транслируется во внутренние настройки программного комплекса. Так мы реализуем информационно–центричный подход к защите, в котором характер и ценность бизнес–данных определяют политики безопасности, реализуемые непосредственно в электронной среде.

ВОПРОС: Насколько установка вашего ПО помешает работе пользователей? Не помешают ли ограничения и блокировки привычной работе?

Во–первых, ограничительные политики не являются искусственно надуманными, они лишь реализуют те требования безопасности, которые ответственный пользователь и ранее должен был соблюдать. А во–вторых, появление небольшой оранжевой метки на электронных конфиденциальных данных облегчит работу пользователей, избавив их от типовых страхов.

Увидев на экране рабочего места файл с защищенной меткой, работник будет знать: файл лежит там, где ему разрешено быть, и ни в каких других местах корпоративной сети, его не откроет никто, кроме уполномоченных лиц, имеющих необходимый допуск, его случайно или злонамеренно не скопируют на флешку, не отправят по почте, не выложат в облако, не вытащат из него текст, чтобы переслать сообщением, все действия с ним учтены и известны. В этом вся разница между работой с конфиденциальными данными и с обычными. ■



perimetrix © 2021 Perimetrix LLC

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.