periметрix

ФОКУС *на* защите

КАК ОБЕЗОПАСИТЬ ДАННЫЕ —
«ШАШЕЧКИ» ИЛИ ЕХАТЬ?

ПРЕЖДЕ ЧЕМ РАССУЖДАТЬ о преимуществах средств борьбы с утечками данных, давайте попробуем встать на место владельца ценного информационного актива и понять его истинные потребности. А поймем мы его достаточно легко, если представим себе «ценный информационный актив», например, в виде новенького личного автомобиля, оставленного вами на стоянке возле крупного торгового центра. Возвращаясь с пакетами из магазина, вы переводите взгляд на то место, где оставили свой автомобиль, и... Какое истинное желание вы испытываете?

- Я бы хотел, чтобы видеокамеры торгового центра оперативно и подробно ***запротоколировали все действия злоумышленников*** по угону моего автомобиля.
- Я бы хотел, чтобы в случае угона рано или поздно ***виновные были найдены*** и понесли наказание.
- Я бы хотел, чтобы в случае угона моей машины мне ***выплатили страховку*** и предоставили такси.

Как вам такие варианты? Вызывают воодушевление? Любой хозяин всем предложенным вариантам предпочтет, чтобы его автомобиль ***остался нетронутым*** там, где он его оставил. То же самое абсолютно верно и в отношении владельцев ценных информационных активов. Данные должны быть защищены так, чтобы они просто не могли «утечь». Это и есть требуемый заказчиком фокус задачи защиты от утечек.

Анатомия утечки

Информация, как объект защиты, в каждый момент времени находится в некоем «*информационном контейнере*», состоянии, предназначенном для ее временного или постоянного хранения. Это может быть бумага, файл на флэшке, мозг человека, облачное хранилище и т.д. С этой точки зрения *утечка* — это не разрешенное политиками безопасности перемещение конфиденциальной информации из легитимного контейнера-источника в нелегитимный контейнер-приемник, либо использование нелегитимного канала передачи, либо обработка ее в нелегитимном узле обработки.

Если смотреть на утечку таким образом, становится понятным, что защищать в компьютерной среде технически возможно только такую информацию, которая принципиально хранится, перемещается и обрабатывается именно в компьютерной среде — базы данных, сложные многослойные графические объекты, чертежи, объемные текстовые, аудио- и видео-данные. Иная, «простая» информация, которую можно подглядеть на экране монитора, подслушать, переписать на клочок бумаги или просто запомнить — не может быть защищена какими-либо программными средствами. Не стоит испытывать иллюзий по этому поводу.

Вам средство борьбы или средство защиты?

Рынок DLP (*Data Leak Prevention*) формировался как альтернатива жестким решениям СЗИ, хорошо реализующим регламенты защиты гостайны, но мало пригодным для работы с гибкой и динамичной коммерческой тайной. Идея контроля трафика по всем возможным каналам коммуникаций с динамической детекцией конфиденциальной информации — сама по себе прекрасна. Поведенческий анализ, построение карты взаимосвязей и вынесение вердиктов о степени лояльности пользователей — блестящая демонстрация возможностей аналитики DLP. Но какое все это имеет отношение к *предотвращению* утечки данных?

Давайте начистоту: любая система, основанная на вероятностных методах определения какая информация нуждается в защите, а какая — нет, **не может защитить** вообще ничего. Она либо выпустит ценную информацию наружу, либо ошибочно заблокирует безобидную рутинную операцию пользователя.

А вот в роли инструмента «Диагностики Лояльности Пользователей», задачей которого является выявление возможных сценариев и потенциальных исполнителей утечек — DLP, безусловно, на своем месте.

Но давайте не путать борьбу с утечками как расследование инцидентов нелояльного поведения сотрудников и защиту от утечек как задачу *сохранения конфиденциальности*, вполне утилитарную и технически выполнимую в отношении определенного класса информационных активов, описанных выше.

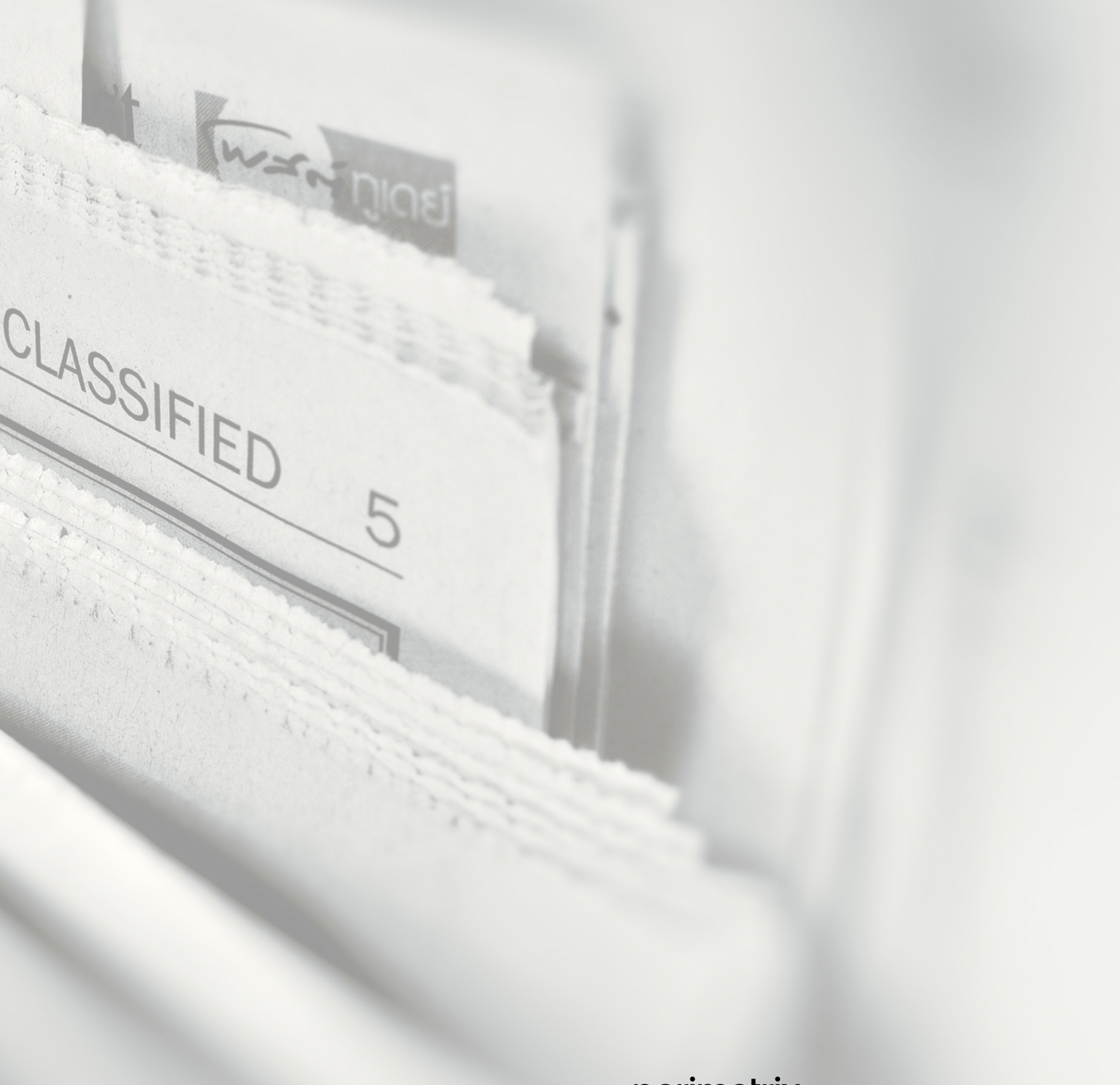
В защиту режима

Принцип защиты ценных данных должен быть прост и категоричен: «*Запрещено все, кроме того, что в явном виде разрешено*». Другими словами, если вы хотите защитить свои ценные данные от утечки, вы должны выполнить несколько последовательных действий.

Во-первых, четко определить, какие данные вы намерены защищать и присвоить этим данным «гриф» (классификационную метку, определяющую уровень доступа). Во-вторых, описать для защищаемых данных разрешенный периметр — допустимые места хранения, каналы для перемещения, программы для обработки, список пользователей с соответствующими уровнями допуска. И третье — программно-техническими инструментами ограничить любые действия, оставшиеся за пределами разрешений вводимого режима. Вот тогда ваши ценные данные **будут защищены.**

Жаль, что в данном случае будет так мало инцидентов для расследования... Но инциденты — это хлеб для средств «борьбы с утечками».

А я бы хотел, чтобы никто чужой не ездил на моем автомобиле, и чтобы он всегда оставался нетронутым там, где я его оставил. ■



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.

© COPYRIGHT. ALL RIGHTS RESERVED

ALL RIGHTS RESERVED. NO PART OF THIS PUBLICATION MAY BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, INCLUDING PHOTOCOPYING, RECORDING, OR OTHER ELECTRONIC OR MECHANICAL METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF THE PUBLISHER, EXCEPT IN THE CASE OF BRIEF QUOTATIONS EMBODIED IN CRITICAL REVIEWS AND CERTAIN OTHER NONCOMMERCIAL USES PERMITTED BY COPYRIGHT LAW.