Защита от инсайдера: интервью Александра Астахова для CNews Analytics

написано GlobalTrust.ru | 10.09.2012

Обычно, самое большое, что можно себе позволить в реальной корпоративной среде, это попытаться обнаружить факт «слива» информации, поймать инсайдера за руку и привлечь к ответственности.

Интервью генерального директора GlobalTrust Александра Астахова для CNews, статья «Борьба с инсайдерами: подбираем амуницию», 6 марта 2007

CNews: Какого рода решения, на ваш взгляд, позволяют наиболее эффективно бороться с инсайдерами?

В GlobalTrust мы сознательно избегаем употребления неудачного маркетингового термина «решение» в данном контексте, т.к. в нашем бизнесе нет готовых решений. Каждая организация и ее потребности в области информационной безопасности индивидуальны. «Решения» нельзя покупать или продавать, и мы видим свою основную задачу как консультанта в том, чтобы помочь руководителям организации самим найти и принять правильное и экономически обоснованное решение.

В своей статье я хотел продемонстрировать многогранность проблемы инсайда и применение комплесного подхода для ее решения. Инсайд — это проблема юридическая, социально-этическая, управленческая и технологическая одновременно. Нам приходится иметь дело с различными типами инсайдеров, имеющих совершенно разную мотивацию, квалификацию и уровень доступа к информации. Задача заключается в том, чтобы для каждого типа инсайдеров подобрать оптимальный набор

защитных мер. Так, например, юридические инструменты не работают, если не удается вовремя обнаружить инсайдера и собрать против него необходимые улики, а традиционные средства защиты от НСД неэффективны против инсайдера, преднамеренно «сливающего» информацию, к которой он имеет легальный доступ.

Обычно, самое большое, что можно себе позволить в реальной корпоративной среде, это попытаться обнаружить факт «слива» информации, поймать инсайдера за руку и привлечь к ответственности. Другими словами, если речь идет о шпионах (самой малочисленной и вместе с тем самой опасной категории инсайдеров), то на первый план выходит не объект защиты (т.к. шпион все-равно найдет способ украсть информацию), а источник угрозы (т.е. обнаружение и нейтрализация самого шпиона). Поэтому особый акцент в статье я сделал на средствах мониторинга действий пользователей корпоративной сети, являющихся по-существу особым классом шпионского ПО, позволяющем бороться со шпионами их же методами.

CNews: Какие средства для обнаружения инсайдеров может предложить компания GlobalTrust?

Для обнаружения исайдеров GlobalTrust предлагает продукты американской компании SpectorSoft Corporation. Флагманский продукт этой компании — Spector 360, в отличие от подавляющего большинства существующих средств мониторинга действий пользователей, является профессиональным продуктом корпоративного уровня, обеспечивающим централизованное развертывание системы, мощные средства администрирования и генерации отчетов, систему оповещений, анализ информации в реальном времени по ключевым словам, поддержку всевозможных коммуникационных протоколов и приложений и т.п. Spector 360 позволяет также контролировать такие немаловажные параметры как производительность труда и компетенция сотрудников. Службы технической поддержки при необходимости могут воспользоваться им для восстановления критичной информации и разобраться в причинах возникновения сбоев, проанализировав какие действия пользователя им предшествовали. Все это в совокупности позволяет гарантировать высокую степень востребованности продукта на современном корпоративной рынке.

CNews: Как решить этические проблемы, возникающие при организации борьбы с инсайдерами?

Конечно, такие меры как мониторинг действий пользователей и фильтрация электронных сообщений не способствуют повышению взаимного доверия между сотрудниками организации и ее руководством, что может служить серьезным демотивирующим фактором. Для того, чтобы избежать морально-этических проблем в коллективе, необходимо четко определить политику в области допустимого использования ресурсов организации и последовательно формировать соответствующую культуру обращения с информацией путем повышения осведомленности сотрудников в вопросах информационной безопасности. Надо научить людей отличать конфиденциальную информацию от открытой, личную информацию от служебной, допустимые действия от недопустимых. Борьба с инсайдерами не должна носить характер доносительства и шпиономании. Инсайд — это проблема всего коллектива, которую нельзя игнорировать. Мониторинг должен быть сосредоточен не на личности отдельных сотрудников, а на потенциально опасных действиях.

CNews: Насколько сильны позиции отечественных разработок в сфере борьбы с инсайдерами по сравнению с западными?

Несомненно существуют интересные отечественные разработки, некоторые из которых были мной упомянуты в статье. Особенно их много в области мандатного управления доступом и криптографии, без которых немыслима реализация мер по защите государственной тайны, а также в области противодействия иностранным техническим разведкам и предотвращения утечки информации по техническим каналам. Однако в бизнес среде многие из этих продуктов и технологий имеют весьма ограниченное применение, так как бизнес в первую очередь озабочен экономической целесообразностью применяемых мер. Что касается продуктов ориентированных на защиту корпоративных сетей, то здесь наблюдается такое же количественное и качественное отставание от запада, как и в областях ИТ и ИБ в целом.

Полный текст статьи: http://safe.cnews.ru/reviews/index.shtml?2007/03/06/238899

GlobalTrust Solutions попытается заработать на комплекте типовых документов по информационной безопасности

написано GlobalTrust.ru | 10.09.2012

Представители индустрии все чаще говорят о необходимости более активного использования в России современных ИТ-стандартов и методологий, активно использующихся на развитых рынках. И некоторые движения на этом фронте уже происходят.

Мало того, подобные **документы становятся товаром**, который заказчикам предлагается приобретать вместе с консалтинговыми услугами. Именно так действуют в GlobalTrust Solutions: компания сообщила о выпуске новой редакции обширного комплекта типовых документов по информационной безопасности на русском языке – GTS 1000.

В комплект входит более 120 документов, которые разбиты на 16 категорий: политики, стандарты, концепции, процедуры, правила, руководства, положения, регламенты, инструкции, реестры, приказы, журналы, планы работ, модели угроз и нарушителей, формы отчетов и проектные документы.

«Разработка пакета документов, аналогичного комплекту GTS 1000 по содержанию, качеству и глубине проработки – длительный и трудоемкий процесс, на который у команды профессионалов, обладающих отличными знаниями международных и отраслевых стандартов и нормативной базы РФ,

уйдет не менее полугода. При этом потребность в подобных документах есть у любой организации, сотрудники которой намерены разработать локальную нормативную базу в области информационной безопасности, внедрить систему управления информационной безопасностью, документировать процессы и требования безопасности, а также распределить роли и назначить ответственных за безопасность в организации», — говорят в GlobalTrust Solutions.

В компании уверяют, что все документы, входящие в комплект, «были опробованы на практике более чем в 100 организациях» и «полностью соответствуют действующей законодательной и нормативной базе РФ в области защиты информации и персональных данных, а также требованиям международных и отраслевых стандартов (например, ISO 27001, СТО БР ИББС и т. д.)».

Одним из главных преимуществ GTS 1000 в GlobalTrust Solutions считают то обстоятельство, что все входящие в комплекта документы являются законченными и, в общем случае, не требуют значительных доработок для начала их использования в конкретной организации (т. е. не являются простыми формами или шаблонами). Кроме того утверждается, что все документы обеспечены не только консалтинговой поддержкой, но и «гарантиями возврата денег».

В GlobalTrust Solutions также обещают, что входящие в комплект документы весьма подробны. Так, план обеспечения соответствия в области персональных данных включает в себя 63 этапа, каждый из которых, по сообщению компании, «расписывается по целям, мероприятиям, нормативным требованиям, исходным данным, результирующим документам, срокам выполнения и ответственности, а также сопровождается поясняющей информацией». В качестве другого примера представители компании приводят типовую частную модель угроз безопасности, которая «не ограничивается только формальными положениями и перечнями угроз, утвержденными регуляторами, а значительно расширяет как общий перечень угроз, так и набор параметров, по которым они оцениваются».

Источник: ibusiness.ru