Сертификация компании CMA по требованиям BS 7799

написано GlobalTrust.ru | 28.09.2012

Российское представительство Британского Института Стандартов совместно с компанией GlobalTrust сообщают о завершении сертификации системы управления информационной безопасностью компании «CMA Small Systems» по требованиям британского стандарта BS 7799 в системе аккредитации UKAS.

Штаб-квартира компании «CMA Small Systems» расположена в Швеции. За последние годы CMA успешно закрепила за собой место надежного поставщика систем и решений под ключ для международной сферы финансовых услуг. Группа CMA представлена в Швеции, России и Франции. Дочерние компании группы CMA поставляют продукты и услуги в сфере управления информационными технологиями, управления активами, в области финансов и лизинга, а также в сфере консалтинга.

Сертификация охватывала российский, шведский и французский офисы компании. В область регистрации вошли процессы разработки, внедрения, сопровождения и технической поддержки разрабатываемого программного обеспечения.

В течение пяти месяцев специалисты CMA при помощи консультантов GlobalTrust осуществляли аудит и документирование процессов управления информационной безопасностью, разработку и внедрение организационно-распорядительных документов и процедур, оценку информационных рисков и планирование мероприятий по построению и внедрению СУИБ. Сотрудники CMA прошли обучение на авторизованных учебных курсах BSI по внедрению и внутреннему аудиту СУИБ в соответствии с требованиями BS 7799.

Сертификационный аудит проводился специалистами российского отделения BSI – BSI SM Russia.

CMA стала первым в России разработчиком программного обеспечения, успешно внедрившим СУИБ в соответствии с BS 7799 и в полном объеме сертифицировавшим основные бизнес процессы по требованиям стандарта. Полученный сертификат является важным показателем надежности компании в глазах клиентов, партнеров, акционеров, аудиторов, и дает возможность CMA успешно конкурировать с ведущими европейскими и американскими компаниями на международном рынке.

«Любая компания в независимости от ее профиля задается вопросом: «Насколько защищена наша информационная система?». Этот вопрос иногда является краеугольным камнем для победы компании в тендере и при заключении контракта. Сертификационный аудит в трех подразделениях CMA подтвердил соответствие внедренной системы требованиям BS 7799, что, безусловно, в свою очередь позволит CMA выйти на другой качественный уровень в работе со своими заказчиками, так как наличие зарегистрированной СУИБ в соответствии с требованиями BS 7799-2:2002 позволяет наглядно показать деловым партнерам, инвесторам и клиентам, что в компании налажено эффективное управление информационной безопасностью и компания обеспечивает способность управлять информационными рисками », — сказала **Наталья Горобец**, Директор департамента по сертификации систем менеджмента BSI MS Russia и ведущий BS 7799 аудитор.

«Процесс сертификации СУИБ в соответствии с требованиями стандарта BS 7799-2:2002 в значительной мере помог нашей компании оценить эффективность управления информационной безопасностью на всех этапах жизни основных бизнес – процессов», — отметил **Владислав Демидов**, начальник отдела информационной безопасности компании CMA Small Systems AB.

«Британский стандарт BS 7799 получает все большее признание в России, как и во всем мире. В том числе, этому способствует распространение русской редакции стандарта, переведенной специалистами GlobalTrust. Мы убеждены, что уже в недалеком будущем наличие сертификата соответствия по ISO 27001 (ИСО версия второй части BS 7799) станет для

большинства российских компаний важным атрибутом, позволяющим продемонстрировать клиентам и партнерам компании наличие эффективной системы управления информационной безопасностью», – отметил **Александр Невский**, руководитель проекта со стороны GlobalTrust.

Защита от инсайдера: интервью Александра Астахова для CNews Analytics

написано GlobalTrust.ru | 28.09.2012

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