УДК 004.683

Печень С.А. (ГУИКТ)

КОНТРОЛЬ КРИТИЧНЫХ БИЗНЕС-ПРОЦЕССОВ СРЕДСТВАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном бизнесе для осуществления контроля за функционированием активно используются информационные технологии, одним из основных элементов которых на современном предприятии является информационная безопасность. Функция контроля применительно к информационной безопасности является такой же важной, как и контроль деятельности предприятия с точки зрения финансов, производства, правовой деятельности, взаимоотношений с клиентами.

В крупных компаниях информационная безопасность (ИБ) воспринимается как часть бизнеса, а процессы обеспечения ИБ стоят в ряду процессов, которые позволяют бизнесу эффективно и непрерывно функционировать. Если контроль за деятельностью предприятия с точки зрения финансов, производства, взаимоотношений с клиентами осуществляется с использованием широко распространенных систем автоматизации типа ERP, CRM и др., то контроль с точки зрения ИБ все еще далек от самого бизнеса и его задач. Данные утверждения наиболее ярко проявляются в тех отраслях, где зависимость бизнеса от ИТ очевидна. Безусловно, одной из первых к такой отрасли можно с уверенностью отнести и телекоммуникационную.

Обратимся к современной практике и выясним, какие критерии рассматривают клиенты при выборе организации и какие риски в настоящее время существуют для телекоммуникационных организаций.

С точки зрения клиента существует перечень важных критериев при осмысленном выборе провайдера услуг связи, как правило от качества услуг которого зависит и в их числе: условия обслуживания, перечень услуг, тарифные сетки лояльности, стоимость обслуживания, качество обслуживания, расположение и количество офисов и др. Такого поставщика услуг связи можно в современных условиях назвать телекоммуникационным партнером. В таком случае очень важно иметь дело с известным и надежным брендом (в том числе с организацией, имеющей развитую инфраструктуру, стабильные и высокие рейтинги).

Современная практика говорит о том, что при выборе следует рассматривать такие аспекты, как качество корпоративного управления и, в частности, риск-менеджмент. Это в первую очередь касается крупных корпоративных бизнес-клиентов. Хотя и о физических лицах не стоит забывать. Вряд ли кто-то захочет иметь дело с предприятием с плохой репутацией. А репутацию испортить гораздо легче, чем восстановить.

Безусловно, одним из факторов риска является мошенничество со стороны собственных сотрудников - инсайдерство. Примеров мошеннических действий со стороны сотрудников можно не приводить, их достаточно описано в прессе. Рейтинговые агентства с легкостью снижают рейтинг надежности при наличии серьезных инцидентов. Государственные регулятивные органы могут отзывать лицензии.

Задача менеджмента организации — «держать руку на пульсе» для обнаружения и предотвращения мошенничества. Конечно, в данном утверждении есть доля лукавства. Ведь для борьбы с мошенничеством есть специально выделенные сотрудники и целые подразделения. Но возникает вопрос, а есть ли у них эффективные инструменты для работы, и может ли руководство адекватно оценить деятельность этих подразделений. Вопрос даже шире — может ли организация в лице своего менеджмента предоставить обоснованные гарантии надежности.

В целом ответить на этот вопрос можно положительно. Но это в теории, а на практике специалисты, отвечающие за вопросы безопасности и противодействия мошенничеству,

заявляют, что отсутствие в бизнес-приложениях средств контроля действий пользователей лишает их возможности действовать эффективно.

Помимо отсутствия адекватных технических средств контроля, о требованиях к которым поговорим позже, существует и проблема в наличии выстроенных процессов управления системой ИБ, включающих, в том числе мониторинг и управление инцидентами. При этом одной из задач подобных процессов является «вертикальная» интеграция исполнителей, ответственных за те или иные задачи (к примеру, обнаружение мошенничества), и руководства, которое должно принимать управленческие решения на основе полученных «снизу» данных.

На практике же информация для принятия управленческих решений может быть просто не получена из-за отсутствия адекватных технических средств (что является основной проблемой на сегодняшней день). Кроме этого высокоуровневые отчеты для руководства могут содержать искаженные факты, так как информация от первичных источников событий будет претерпевать ряд преобразований и обобщений. Причем искажения могут быть как умышленного, так и непредумышленного характера (в том числе и различия в интерпретации одинаковых фактов разными людьми). Да и время доведения необходимой информации до руководства может быть чрезмерно велико, что приводит к задержке в принятии важных решений.

В результате руководство не имеет возможности контролировать важные процессы обеспечения ИБ и противодействовать мошенничеству. Это приводит к тому, что организация не может «с чистой совестью» гарантировать клиентам надежность и безопасность клиентских средств.

Но если даже в настоящее время организация не задумывается (хотя кризис к этому подталкивает) о серьезности подхода к вопросам ИБ, то существуют государственные(НД ТЗИ) и отраслевые стандарты (ISO). В настоящее время различные стандарты, законы, отраслевые требования в области информационной безопасности призваны защитить бизнес-процессы предприятия, а значит и интересы клиентов, инвесторов, партнеров по бизнесу.

По сути, все современные стандарты говорят одно и то же: топ-менеджеры должны участвовать в процессах обеспечения и управления ИБ, необходимо оценивать риски и управлять инцидентами, необходимо планировать и реализовывать меры по обеспечению непрерывности бизнеса и т.д.

Один из основных вопросов, который затрагивается в стандартах, — создание системы менеджмента ИБ (СМИБ), включающей контроль эффективности используемых средств защиты и процессов СМИБ. Кроме того, в современных стандартах все больше внимания уделяется требованиям к обеспечению контроля действий пользователей в бизнес-системах. И вновь мы приходим к проблемам, рассмотренным ранее.

Ущерб, который может быть нанесен предприятию при невыполнении требований регулирующих органов, различен: начиная от небольших штрафов (к примеру, при невыполнении требований по радиоизлучающим приборам) и заканчивая невозможностью предоставлять тот или иной вид услуг (защищенные узлы доступа).

Для обеспечения контроля необходимы эффективные процессы системы менеджмента ИБ (СМИБ), а также технические средства обеспечения контроля действий пользователей.

В отношении процессов СМИБ (а это в первую очередь процессы, связанные с контролем эффективности и управлением инцидентами) можно смело обращаться к развитым западным стандартам, актуальным в том числе и на Украине:

- ISO/IEC 27001:2005 (Требования к системе менеджмента ИБ);
- ISO/IEC 18044:2004 (Управление инцидентами ИБ);

Целью СМИБ по большому счету является создание зрелой системы менеджмента ИБ, интегрирующей в процессы обеспечения ИБ как ИТ-подразделения, подразделения

информационной безопасности, внутреннего контроля, так и бизнес-подразделения (включая топ-менеджеров).

Говоря о второй составляющей — технических средствах, стоит еще раз обратить внимание на то, что современные бизнес-приложения в большинстве своем не имеют требуемого полного функционала. Общие требования к средствам контроля действий пользователей можно выразить следующим образом:

- независимость от бизнес-приложения;
- контроль действий всех пользователей;
- возможность использования специальными подразделениями (информационной безопасности, внутреннего контроля) независимо от IT-подразделения;
- наличие развитых средств моделирования схем мошенничества;
- возможность работы, как в режиме реального времени, так и с журналированными событиями;
- функционал оповещений;
- отчетность различного уровня (в том числе и для руководства);
- средство автоматизации расследования инцидентов и контроля хода расследования (в том числе руководством).

Вспользующие их компании получают следующие выгоды:

- возможность обнаружения мошеннических действий на основе гибко настраиваемых сценариев;
- сокращение времени расследования инцидентов, связанных с мошенничеством;
- получение объективной информации о произошедших инцидентах на всех уровнях корпоративного управления.

Подобные средства не являются традиционными и не так распространены, тем не менее широкое внедрение данных систем во всем мире говорит об их эффективности и пользе для бизнеса.

Наличие выстроенных процессов СМИБ в сочетании с эффективными средствами автоматизации этих процессов может являться тем самым фактором, который даст гарантию как руководству, так и клиентам (инвесторам, партнерам) в том, что все в вашей организации под контролем.

Список литературы

1. Хорошко В.А., Чекатков А. А. Методы и средства защиты информации/Под. ред. Ю.С. Ковтанюка. - К.:Юниор, 2003.- 504 с.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.- К.:ООО «ДС», 2001.-688 с.

3. С.А. Печень. Корпоративная безопасность при доступе сотрудников к наиболее популярным ресурсам сети интернет-ДУІКТ, 2008. – с.65-71.

В статье рассматриваются актуальные не только во время кризиса аспекты создания системы менеджмента ИБ (СМИБ), включающей контроль эффективности используемых средств защиты и процессов СМИБ.

Ключевые слова: критичные бизнес-процессы, контроль эффективности.

У статті розглядаються актуальні не тільки під час кризи аспекти створення системи менеджменту ІБ (СМІБ), що включає контроль ефективності використовуваних засобів захисту і процесів СМІБ.

Ключові слова: критичні бізнес-процеси, контроль ефективності.

In article are considered actual not only during crisis aspects creation of management system of the information security including the control of used protection efficiency frames and it processes.

Key words: critical business-process, efficiency control.

Поступила 9.09.2009