«Витрина магазина»

бизнес предусматривает обмен транзакциями с клиентами, отношения могут длиться недолго, ценность любой транзакции ограничена.

«Сервисы, предоставляемые по подписке» бизнес предполагает установление длительных долгосрочных взаимоотношений с клиентом.

Данные носят постоянный характер, доступ к другим бизнес-системам ограничен, проблемы сохранения конфиденциальности и разделения данных становятся более сложными.

«Устройства специального назначения» бизнес предлагает ощутимые ценности клиенту с помощью точек доступа специального назначения.

Доступ к остальным бизнес-системам ограничен в силу того, что точка доступа является устройством с ограниченной функциональностью. Физическая защита устройства доступа — еще один предмет заботы, когда речь заходит о безопасности.

«Сотрудник—бизнес»

Сотрудник (в данном контексте — потребитель) может сидеть в корпоративной инфраструктуре, повышая риски для безопасности компании в силу доступа к дополнительным системам.

Конфиденциальность данных, фигурирующих во взаимоотношениях между сотрудником и бизнесом, должна быть обеспечена с помощью надлежащих элементов управления доступом и контроля за разделением данных.

Фундаментальными характеристиками **B2C** являются два момента:

- во-первых, необходимость сбора данных о пользователе с помощью некоторого процесса регистрации;
- во-вторых, ограниченность механизмов аутентификации идентификационных данных о пользователе.

Основными **угрозами** модели **B2C** являются:

- ложная идентификация;
- сопутствующий доступ к бизнес-системам;
- ненадлежащее использование персональных данных.

Атаки, проистекающие из этих угроз, могут зарождаться как внутри бизнеса, так и извне его.

Для модели **B2C** предусматриваются следующие меры противодействия названным угрозам:

- антивирусные технологии;
- управление доступом;
- управление аутентификацией;
- управление авторизацией;
- управление конфиденциальностью;
- системы обнаружения вторжений;
- межсетевые экраны;
- зашифрованные транзакции.

«Бизнес-бизнес»

Взаимодействие «Бизнес—бизнес» **(B2B)** предусматривает выполнение защищенных коммерческих транзакций между двумя и более организациями.

Стороны в явной или скрытой форме понимают возможные риски, методы их нейтрализации и ответственность каждой из сторон.

Цель модели «Бизнес-бизнес» состоит в том, чтобы обеспечить эффективный и безопасный обмен информацией между сторонами в контексте доверительных взаимоотношений.

Существуют три категории взаимоотношений «Бизнес—бизнес»:

1. «Простой поставщик»
2. «Доверенный поставщик»
3. «Партнерство».

«Простой поставщик»

Один бизнес связывается с другим бизнесом с целью совершения бизнес-транзакций. Совместно используемые данные не носят слишком чувствительного характера, поэтому их можно не шифровать. Система безопасности, являющаяся встроенным атрибутом взаимосвязей **B2B**, служит для защиты точки входа в бизнес от нежелательных попыток вторжения или проникновения вредоносного кода в корпоративную инфраструктуру.

«Доверенный поставщик»

Чувствительность данных возрастает.

В качестве примера можно привести больницу, передающую конфиденциальные медицинские данные о пациенте в страховую компанию. В ходе транзакции одному бизнесу может понадобиться доступ к данным, находящимся в системе, которая принадлежит другому бизнесу. В силу этого обстоятельства может возникнуть необходимость в использовании средств авторизации и управления доступом, а также механизмов аудита.

«Партнерство»

Собственные данные бизнесов становятся данными общего пользования.

Совместное использование данных, характерное для этого вида взаимосвязей между бизнесами, делает инфраструктуру ИТ более подверженной различным угрозам безопасности.

Групповые компоненты безопасности, которые можно использовать для осуществления контрмер, относятся:

- системы обнаружения вторжений;
- межсетевые экраны;
- системы авторизации и управления доступом;
- инструменты разделения контента.

«Операционная безопасность»

Модель «Операционная безопасность» охватывает внутренние компоненты информационных технологий: программное обеспечение, платформы, сетевую инфраструктуру.

Цель операционной безопасности заключается в том, чтобы обеспечить соответствие внутренних систем и инфраструктур бизнеса требуемым уровням безопасности.

Модель «Операционная безопасность» делится на следующие подкатегории:

- **«Пользователи»;**
- **«Децентрализованная инфраструктура»;**
- **«Центры обработки данных»;**
- **«Коммуникации»;**
- **«Производство».**

Дифференцирование этих категорий осуществляется по таким атрибутам, как риски, угрозы, уязвимости и соответствующие им факторы нейтрализации.

«Высокий уровень контроля»

Системы с высоким уровнем контроля (High Assurance Systems) используются в тех случаях, когда бизнесу необходима уверенность в безопасности и доступности критичных систем. Потребность в создании систем с высоким уровнем контроля может возникнуть в связи с высокой чувствительностью/ценностью активов, доверенных информационной системе.

Характеристики системы с высоким уровнем контроля:

- может предотвратить несанкционированные раскрытие, модификацию и «придерживание» чувствительной информации;
- работает в реальном времени: дает результаты в течение заданных временных интервалов;
- обладает выживаемостью: продолжает выполнять свою миссию даже при наличии атак, инцидентов и сбоев;
- является устойчивой к сбоям: гарантирует определенное качество сервиса, невзирая на различные ошибки, например аппаратные сбои, ненормальную нагрузку или аномальные условия работы;
- является защищенной: предотвращает нежелательные события, которые могут привести к смерти, травмам или заболеваниям сотрудников или нанесению ущерба собственности.

Модель «Системы с высоким уровнем контроля» делится на три подкатегории:

- «Условия анклава»
- «Замкнутая среда» (Bounded Environment)
- «Незамкнутая среда»

Бизнес может располагать замкнутыми и анклавными средами, изолированными от недоверенной сети.

Модели безопасности бизнеса в действии:

Widgets, Inc.

В этом разделе рассказывается о том, как вымышленная компания, Widgets, Inc., использует преимущества различных моделей для совершенствования бизнес-процессов, повышения эффективности взаимодействия с партнерами и заказчиками, а также о том, как компания предоставляет сервисы своим сотрудникам.

Widgets, Inc является ведущим поставщиком различных «штучек» (widgets) на мировом рынке.

Данная компания взаимодействует по вопросам бизнеса с целым рядом людей и бизнеса организаций в процессе производства продуктов и доставки их потребителям.

Widgets использует богатые возможности сети Интернет для расширения своего бизнеса. Новые способы взаимодействия, системы и процессы позволяют существенно увеличить продуктивность, но, с другой стороны, они же создают дополнительные возможности для хакеров.

Widgets реализовала присутствие в **Web**, позволяющее пользователям в любой точке мира познакомиться с информацией о компании.

Эта информация может быть интересна заказчикам, инвесторам и потенциальным сотрудникам. Присутствие в Web формирует достойный имидж компании. Имидж, представленный в сети Интернет, является важнейшим компонентом имиджа торговой марки, поэтому защита доступности и целостности данных имеет большое значение.

Widgets является надежным поставщиком продукции для нескольких крупных бизнес-партнеров.

Компания использует модель B2B для организации массовых поставок своих продуктов.

Это позволяет **Widgets** оперативно реагировать на изменившиеся потребности заказчиков.

Сегодня для компании **Widgets** внедрить систему с высоким уровнем контроля не представляется возможным из-за ее высокой стоимости.

Однако в **Widgets** предвидят времена, которые потребуют реализации функций безопасности гораздо более высокого уровня для критичных систем.