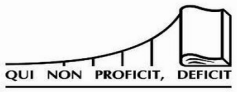

МОСКОВСКИЙ УНИВЕРСИТЕТ ИМ. С.Ю.ВИТТЕ

Кафедра информационных систем

Рейтинговая работа Реферат

(домашняя творческая работа, расчетно-аналитическое задание, реферат, контрольная работа)

по дисциплине Информационные системы и технологии

Задание/вариант № 3

Тема* Какие бы правила Вы внедрили в организации для обеспечения информационной безопасности.

Выполнена обучающимся группы о.ИЗДтс 30.2/Б-20

Цуренкова Татьяна Евгеньевна

(фамилия, имя, отчество)

Преподаватель

_____

(фамилия, имя, отчество)

Москва – 2020 г.

Оглавление

Введение

Архитектура корпоративной информационной безопасности (EISA)-это практика применения всеобъемлющего и строгого метода описания текущей и/или будущей структуры и поведения процессов безопасности организации, систем информационной безопасности, персонала и организационных подразделений таким образом, чтобы они соответствовали основным целям и стратегическому направлению организации.

Хотя она часто ассоциируется строго с технологией информационной безопасности, она более широко относится к практике безопасности оптимизации бизнеса в том смысле, что она также касается архитектуры безопасности бизнеса, управления производительностью и архитектуры процессов безопасности.

Архитектура корпоративной информационной безопасности становится общепринятой практикой в финансовых институтах по всему миру. Основной целью создания архитектуры информационной безопасности предприятия является обеспечение согласованности бизнес-стратегии и ИТ-безопасности. Таким образом, архитектура информационной безопасности предприятия позволяет проследить весь путь от бизнес-стратегии до базовой технологии.

Архитектура корпоративной информационной безопасности впервые была официально позиционирована компанией Gartner в своем техническом документе под названием “включение безопасности в процесс корпоративной архитектуры”. Это было опубликовано 24 января 2006 года. Со времени этой публикации архитектура безопасности перешла от архитектуры, основанной на силосе, к корпоративному решению, которое включает в себя бизнес, информацию и технологии.

Бизнес-архитектура, информационная архитектура и технологическая архитектура раньше назывались сокращенно бит. Теперь, когда безопасность стала частью архитектурного семейства, она стала битами.

Какие бы правила Вы внедрили в организации для обеспечения информационной безопасности

Архитектура корпоративной информационной безопасности впервые была официально позиционирована компанией Gartner в своем техническом документе под названием “включение безопасности в процесс корпоративной архитектуры”. Это было опубликовано 24 января 2006 года. Со времени этой публикации архитектура безопасности перешла от архитектуры, основанной на силосе, к ориентированному на предприятие решению, включающему бизнес, информацию и технологии.

Он также отражает новое дополнение к семейству архитектуры Enterprise под названием "Безопасность". Бизнес-архитектуру, информационную архитектуру и технологическую архитектуру раньше называли сокращенно бит. Теперь, когда безопасность стала частью архитектурного семейства, она стала битами.

Императивы изменения архитектуры безопасности теперь включают в себя такие вещи, как

- Бизнес-планов;
- Законодательные и правовые требования;
- Технологические дорожные карты;
- Отраслевые тенденции;
- Тенденции риска;
- Провидцы.

Цели:

Обеспечение структуры, согласованности и связности.

Необходимо включить выравнивание бизнеса и безопасности.

Определение сверху вниз, начиная с бизнес-стратегии.

Убедитесь, что все модели и реализации могут быть прослежены до бизнес-стратегии, конкретных бизнес-требований и ключевых принципов.

Обеспечить абстракцию таким образом, чтобы усложняющие факторы, такие как география и технологическая религия, могли быть удалены и

восстановлены на различных уровнях детализации только тогда, когда это необходимо.

Установить общий "язык" информационной безопасности внутри организации

Методология:

Практика архитектуры информационной безопасности предприятия включает в себя разработку структуры безопасности архитектуры для описания ряда "текущих", "промежуточных" и "целевых" эталонных архитектур и применение их для согласования программ изменений. Эти структуры подробно описывают организации, роли, сущности и отношения, которые существуют или должны существовать для выполнения набора бизнес-процессов. Эта структура обеспечит строгую таксономию и онтологию, которая четко определяет, какие процессы выполняет бизнес, и подробную информацию о том, как эти процессы выполняются и обрабатываются. Конечный продукт - это набор артефактов, которые с разной степенью детализации описывают, что именно и как работает бизнес и какие меры безопасности требуются. Эти артефакты часто являются графическими.

Учитывая эти описания, уровень детализации которых будет варьироваться в зависимости от доступности и других практических соображений, лицам, принимающим решения, предоставляются средства для принятия обоснованных решений о том, куда инвестировать ресурсы, где перестраивать организационные цели и процессы, а также какие политики и процедуры будут поддерживать основные миссии или бизнес-функции.

Сильный процесс архитектуры корпоративной информационной безопасности помогает ответить на такие основные вопросы, как:

Какова степень риска информационной безопасности Организации?

Поддерживает ли текущая архитектура безопасность организации и повышает ли она ее ценность?

Как можно изменить архитектуру безопасности, чтобы она добавляла больше ценности оргизации?

* Исходя из того, что мы знаем о том, чего организация хочет достичь в будущем, будет ли текущая архитектура безопасности поддерживать или препятствовать этому?

Внедрение архитектуры корпоративной информационной безопасности обычно начинается с документирования стратегии организации и других необходимых деталей, таких как место и способ ее работы. Затем процесс сводится к документированию отдельных ключевых компетенций, бизнес-процессов и того, как организация взаимодействует сама с собой и с внешними сторонами, такими как клиенты, поставщики и государственные структуры.

Документировав стратегию и структуру организации, процесс архитектуры затем переходит в дискретные компоненты информационных технологий, такие как:

Организационные схемы, виды деятельности и потоки процессов работы ИТ-организации • ;

Организационные циклы, периоды и сроки;

Поставщики технологического оборудования, программного обеспечения и услуг;

Инвентаризация и диаграммы приложений и программного обеспечения;

Интерфейсы между приложениями - то есть: события, сообщения и потоки данных;

Интранет, Экстранет, Интернет, электронная коммерция, ЭОД-связи со сторонами внутри и за пределами организации;

Классификации данных, базы данных и вспомогательные модели данных;

Оборудование, платформы, хостинг: серверы, сетевые компоненты и устройства безопасности и места их хранения;

Локальные и глобальные сети, схемы подключения к интернету.

Там, где это возможно, все вышеперечисленное должно быть непосредственно связано со стратегией, целями и операциями организации. Архитектура информационной безопасности предприятия будет документировать текущее состояние технических компонентов безопасности, перечисленных выше, а также желаемое будущее состояние идеального мира (архитектура ссылок) и, наконец," целевое " будущее состояние, которое является результатом инженерных компромиссов и компромиссов. идеал. По сути, результатом является вложенный и взаимосвязанный набор моделей, обычно управляемых и поддерживаемых специализированным программным обеспечением, доступным на рынке.

Такое исчерпывающее отображение ИТ-зависимостей имеет заметные совпадения как с метаданными в общем смысле ИТ, так и с концепцией ITIL базы данных управления конфигурациями. Поддержание точности таких данных может быть серьезной проблемой.

Вместе с моделями и диаграммами идет набор лучших практик, направленных на обеспечение адаптивности, масштабируемости, управляемости и т. д. Эти лучшие практики системной инженерии не являются уникальными для архитектуры информационной безопасности предприятия, но тем не менее имеют важное значение для ее успеха. Они включают в себя такие вещи, как компонентизация, асинхронная связь между основными компонентами, стандартизация ключевых идентификаторов и т. д.

Успешное применение архитектуры информационной безопасности предприятия требует соответствующего позиционирования в организации. В этой связи часто используется аналогия с градостроительством, и она носит конструктивный характер.

Промежуточным результатом архитектурного процесса является всесторонняя инвентаризация стратегии бизнес-безопасности, процессов бизнес-безопасности, организационных схем, технических описей

безопасности, системных и интерфейсных диаграмм, сетевых топологий и явных взаимосвязей между ними. Описи и диаграммы - это всего лишь инструменты, поддерживающие принятие решений. Но этого недостаточно. Это должен быть живой процесс.

Организация должна разработать и внедрить процесс, обеспечивающий непрерывное движение от текущего состояния к будущему. Будущее состояние, как правило, представляет собой комбинацию одного или нескольких состояний.

Устранение пробелов, существующих между текущей стратегией организации и способностью аспектов ИТ-безопасности поддерживать ее.;

Устранение пробелов, существующих между желаемой будущей стратегией организации и способностью аспектов безопасности поддерживать ее;

Необходимые обновления и замены, которые должны быть внесены в архитектуру ИТ-безопасности на основе жизнеспособности поставщиков, возраста и производительности аппаратного и программного обеспечения, проблем с производительностью, известных или ожидаемых нормативных требований и других проблем, явно не обусловленных функциональным управлением организации • ;

На регулярной основе текущее состояние и будущее состояние пересматриваются с учетом эволюции архитектуры, изменений в организационной стратегии и чисто внешних факторов, таких как изменения в технологии и требованиях клиентов/поставщиков/правительства, а также изменения как внутренних, так и внешних ландшафтов угроз с течением времени.

Фреймворки архитектуры корпоративной информационной безопасности - это всего лишь подмножество фреймворков корпоративной архитектуры. Если бы нам пришлось упростить концептуальную абстракцию архитектуры корпоративной информационной безопасности в рамках общей

структуры, то изображение справа было бы приемлемо в качестве структуры концептуальной архитектуры безопасности высокого уровня.

Другими фреймворками открытой корпоративной архитектуры являются:

Структура и методология SABSA;

Архитектурная структура Министерства обороны США (DoD) (DoDAF);

Extended Enterprise Architecture Framework (E2AF) отинститутапредпринимательства;

Развитие Архитектуры;

Федеральная корпоративная архитектура правительства Соединенных Штатов (FEA);

Интегрированная архитектура Capgemini;

Архитектурная структура Министерства обороны Великобритании (MOD) (MODAF);

Структура корпоративной архитектуры NIH;

Открытая Архитектура Безопасности;

Архитектурная структура предприятия по обеспечению информационной безопасности (IAEAF);

Сервис-ориентированная структура моделирования (SOMF);

Платформа архитектуры открытых групп (TOGAF);

Фреймворк Захмана;

Корпоративная Кибербезопасность (Книга).

Архитектура информационной безопасности предприятия является ключевым компонентом процесса управления технологиями информационной безопасности в любой организации значительного размера. Все больше и больше компаний внедряют формальный процесс архитектуры корпоративной безопасности для поддержки управления и управления ИТ.

Однако, как отмечалось во вступительном абзаце этой статьи, он идеально относится более широко к практике оптимизации бизнеса,

поскольку он также касается архитектуры безопасности бизнеса, управления производительностью и архитектуры безопасности процессов. Архитектура корпоративной информационной безопасности также связана с управлением портфелем ИТ-безопасности и метаданными в корпоративном ИТ-смысле.

В ходе нашего анализа мы выяснили, что частичные методы могут быть в основном разделены на категории:

- управление политиками безопасности и конфигурациями;
- безопасность корпоративных услуг;
- управление ролями безопасности и контроль доступа;
- оценка безопасности и разработка требований.

Однако по причинам, упомянутым ниже, основное внимание в этой статье уделяется целостным структурам. Эксплицируются наиболее важные целостные фреймворки, включая Gartner, SABSA, RiseFramework, AGM-модель и интеллектуальную сервис-ориентированную EISA.

Наиболее известным фреймворком является Gartner, который первым определил термин EISA в работе [4]. Gartner рассматривает совместимость EISA с программой EA и настаивает на сотрудничестве между ними [3]. Следующая видная структура-это SABSA [5] и [6]. Она сделала самую выдающуюся попытку в области целостного EISA. Это многоуровневая архитектура, сопровождаемая методологией реализации.

Подъем-это еще одна важная основа. Это основанный на угрозах и управлении рисками метод, который был внедрен для управления информационной безопасностью на предприятии. Модель управления безопасностью SOAE на основе AGM была создана с использованием двух важных стандартов информационной безопасности, а именно ISO/IEC 17799 и SOGP в модели гибкого управления. Интеллектуальная сервис-ориентированная EISA [2]-это многоуровневая интеллектуальная сервис-ориентированная архитектура для систематического и интеллектуального управления деятельностью EISA. Кроме того, ISO27002 был использован для

выбора услуг информационной безопасности и осуществления управления рисками.

Интероперабельность-это основное внимание в следующем разделе. Из пяти аспектов интероперабельности мы выбрали три наиболее актуальных.

Эти три аспекта-технический, организационный и семантический. Поскольку интероперабельность-это широкое понятие, мы ограничимся обсуждением целостных структур и моделей. В этой связи мы оцениваем эти подходы с точки зрения упомянутых аспектов интероперабельности. Наконец, результаты сравнения представлены в последнем разделе.

Было предпринято много усилий для внедрения архитектурных фреймворков или эталонных моделей корпоративной информационной безопасности. Различие в масштабах и целях этих подходов, а также отсутствие обзоров и дискуссий затрудняют анализ и оценку этих подходов. Упомянутая проблема побудила нас классифицировать эти модели и фреймворки. Мы разработали два аспекта этой классификации.

Эти аспекты-уровень абстракции (целостный или частичный) и архитектурная точка зрения (управленческая или техническая). Как уже говорилось, архитектурная точка зрения (управленческая или техническая) выходит за рамки данной статьи. Соответственно, мы рассматривали доступные методы только с уровня абстракции (целостный VS. частичный) аспект.

1.1. Целостный и Частичные подходы

В прошлом информационная безопасность рассматривалась как незначительная и второстепенная проблема; угрозы создавали низкие риски для информации предприятия. Таким образом, интеграция частичных решений безопасности представлялась достаточной для борьбы с указанными угрозами и установления информационной безопасности на всем предприятии. Все более широкое использование ИКТ предприятиями привело к широким побочным эффектам и появлению новых проблем, решение которых не было найдено в интеграции частичных подходов.

Решение этих новых проблем, безусловно, послужило стимулом для развития подходов с нисходящими перспективами, которые изучают проблемы с более высокого уровня абстракции. В дополнение к упомянутому стимулу три фактора еще более ускорили развитие целостных подходов:

1-разделение инициатив стратегического планирования и решений по обеспечению безопасности решения и мероприятия, которые привели к несовместимости при применении частичных решений по обеспечению безопасности.

2 - функциональное перекрытие между частичными решениями безопасности, что привело к снижению производительности.

3-неполный охват информационной безопасности на предприятии.

Ожидается, что корпоративная информационная безопасность будет соответствовать новым требованиям и реагировать на новые угрозы и опасности. Это подчеркивает необходимость рекурсивных решений, состоящих из последовательных фаз. Никакие частичные подходы не поддерживают измерение времени. Однако несколько целостных подходов поддерживают это измерение.

Заключение

Оценка рисков по критически важным информационным технологическим активам Университета Айовы проводится на регулярной основе как департаментом внутреннего аудита Университета Айовы, так и Управлением государственного аудитора. Обратная связь включает в себя всеобъемлющий отчет о практических рекомендациях по смягчению/устранению рисков.

Управление информационной безопасности и политики также проводит оценку технических рисков и / или тесты на проникновение для руководства и владельцев бизнеса по запросу, которые проводятся и поддерживаются в строго конфиденциальном порядке. Кроме того, существует формализованный процесс утверждения планов ИТ-безопасности для исследований, предшествующих (контрактным) соглашениям, грантам и другим отношениям или сотрудничеству с университетом Айовы, который включает в себя этап оценки рисков безопасности.

Управление информационной безопасности и политики совместно с Комитетом по управлению рисками информационной безопасности и политикой будут, кроме того, содействовать проведению оценки рисков безопасности в масштабах всей организации, когда это необходимо, когда происходят значительные изменения в вычислительной среде, или как минимум в течение пяти лет.

Безопасность должна быть рассмотрена с самого начала любого проекта в университете, а не что-то, что добавляется позже. Управление информационной безопасности и политики-это ресурс, доступный для оказания помощи в этих усилиях на протяжении всего этапа планирования проекта. Кроме того, перед внедрением компьютерных систем, в которых

хранится или обрабатывается конфиденциальная институциональная информация, следует провести контрольную проверку.

Список использованных источников

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2018. — 136 с.

2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.

5. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 с.

6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.

7. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

8. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.