Аналитический отчет по тестовым кейсам:

Замечание: требуются дополнительные сопроводительные комментарии к тексту. При необходимости готов сделать более детальные пояснения в видео презентации и сопроводительных материалов типа структурированных схем в формате BPMN. Также на базе вводной информации и возможных угроз, рисков, - описывается базовая модель, которая присуща данным ситуациям в классическом понимании. Из задания приводится понимание, что есть уязвимости со стороны интеграционных стыков и рассматривается минимальная безопасность с этой точки зрения.

Тестовые кейсы:

1. Вы обнаруживаете админскую консоль веб-сайта Компании, зарегистрированной в Евросоюзе, которая доступна неограниченному кругу лиц в сети Интернет. С помощью её интерфейса доступны на просмотр записи с запросами о приобретении продукции, которые содержат персональные данные лиц, запрашивающих продукцию, а также их коммерческие предложения (что хотят купить, в каком объёме и за сколько). Также в данном интерфейсе доступны логи, в которых видны ip-адреса администраторов Компании, обращавшихся к данной странице.

Вопросы:

a) Как вы презентуете топ-менеджеру без бэкграунда в ИТ/ИБ данную ситуацию в части обнаруженных вами недостатков, присущих ей рисков и рекомендаций? Кто будет указан ответственными сторонами по обозначенным рекомендациям?

Ответ можно предложить в формате, который вы считаете наиболее оптимальным (слайды, текст, …) и с той степенью детализации, которую вы считаете необходимой.

b) Какие меры по митигации рисков вы предложите и как их приоритизируете по двум группам (срочные меры и несрочные меры) для специалистов и менеджеров ИТ и ИБ?

Ответ нужно предложить в текстовом формате.

Ответ:

a) Обнаружена уязвимость доступности панели администратора сайта из вне корпоративной сети, которая позволяет реализовать утечку информацию являющей коммерческой тайной организацией, персональным данным пользователей, отношениям между организациям, специальным предложения и иной чувствительной информации, что может повлечь за собой коммерческие, финансовые, страховые риски, которые могут вылиться в непосильные убытки, атаку на инфраструктуру организации, ее шифрованию, вымогательству. Эта уязвимость реализуется из-за возможности доступа с любого удаленного соединения путем перебора пароля и недостаточной аутентификации/верификации пользователя, путем использования специальных векторов атак через код и инъекции в коде, позволяет сделать закладки вредоносного кода и прослеживать информацию внутри организации, раскрыть торговую и экономическую информацию и многое другое. То есть возможен критичный риск компрометации данных сделок и последующее понесение ущерба компании, упущения экономической выгоды и недополученной прибыли, штрафов со стороны регуляторов и действующего законодательства, в том числе репутационных. Это влечет за собой высокую степень риска и ответственности. В данном случае также раскрываются процессы по социальной инженерии и получении компрометирующей информации для организации, вплоть до орг штатной структуры. В данном случае в блоке digital и отделом ИБ не был проведен аудит и идентификация проблем. Рекомендуется перенести публикацию панели администратора внутри сети и после этого использовать рекомендации в процессах по следующим методическим указаниям: классификатор рисков с рекомендациями и примерами по критическим угрозам безопасности (OWASP TOP 10), основного стандарта подтверждения безопасности приложения (ASVS), использовать модель обеспечения безопасности программного обеспечения, методику оценки рисков (OWASP Risk Assessment Framework), использовать безопасные библиотеки при разработке (NVD), также исключить критичность по уязвимостям (CWE-564, 77, 287, 384, 327, 319, 611, 79, 502) со смежными рекомендациями, также использовать технический набор средств и мер, которые переданы ответственной команде с детализацией технической составляющей. Требуется включение в ДИ ответственности за конкретный функционал, закрепленный за конкретной командой и лицом, которые занимаются обслуживанием сервиса и описать их kpi по обслуживанию сайта. Рекомендована оценка объёма работ и последующая ее

приоритезация для устранения совокупных рисков после первичного устранения доступности сайта в интернете. Далее следует журналировать события и проводить мониторинг.

b) В первую очередь нельзя передавать риск со стороны бизнеса на хостинг провайдера или иное лицо, а следует принять возможные риски описанные в пункте а), по факту уже достигнутых результатов. В данной ситуации следует произвести управление последствиями, чтобы нивелировать воздействие на инфраструктуру и произвести рекомендованные работы по их устранению - самым первым действием устранить публикацию в сети интернет. Избежать риск нет возможности. в следствие чего используются по рекомендациям формат управления вероятностью – которая позволит снизить в последствие возможность реализации рисков, которые были уже допущены. Далее приводится описание в [Таблица 1] по решению задачи с некоторыми допущениями, так как список не конечный.

Срочные меры	Несрочные меры
Перенести публикацию внутри инфраструктуры и выделить конкретные порты по привязанным автогенерируемым ссылкам для входа в панель администратора по двухфакторной авторизации	Внедрить анализатор кода для репозитория и процессов в pipeline ci/cd
Разделить внутри инфраструктуры хранение БД и сделать ее реплицирование, вынести в асинхронное шифрование	Реализовать систему jwt-токенов с кешированием и солью, предусмотрев сессию длиной в 15 минут на стороне frontend-приложения
Произвести настройку WAF по ACL для портов 43, 8080, 72, 883	Реализовать единую точку входа SSO
Реализовать подключение к серверам на базе SSH с использование GPG	Провести модернизацию микро-сервисной архитектруры и исключить элементы, которые «смотрят» в интернет
Изменить ip-адреса подключения к действующим сессиям	Разнести json-элементы в неявный вид и зашифррвать, как и каналы соединения с сервером
Проинформировать пользователей о изменение политики доступности сервисов	Небезопасная десериализация
Провести аналитику по возможным допущенным инцидентам и в отношении к чувствительной информации	«Белые списки» внутри сервера приложения и БД
Изучить векторы атак по OSINT и доступности из интернета по доменам и связанным сущностям сабдоменов (субдоменов)	Внедрить практику pentest
Отключить временно возможность соединения с сервисом существующих учетных данных	На стороне backend предусмотреть проверку по словарям паролей
Изучить последние подключения к панели администратора и посмотреть передаваемые пакеты	Предусмотреть возможность журналирования событий за доверенными пользователями
Изучить возможность передачи данных третьим лицам через почту и внутри инфраструкты	Менять пароль и токен авторизации внутри панели администратора раз в сутки, провести его кеширование, без использования генератора паролей
Осуществить подключение к коннекторам только изнутри инфраструктуры	Автоматизировать скрипты по DDOS, XSS, XML
Изучить возможные последствия доступности к КТ, ПДн внутри инфраструктуры	Реализовать honey - поты для выявления интереса злоумышленников и частоты запросов

Далее приводится описание по (Рисунок 1), который описывает концептуальный подход.

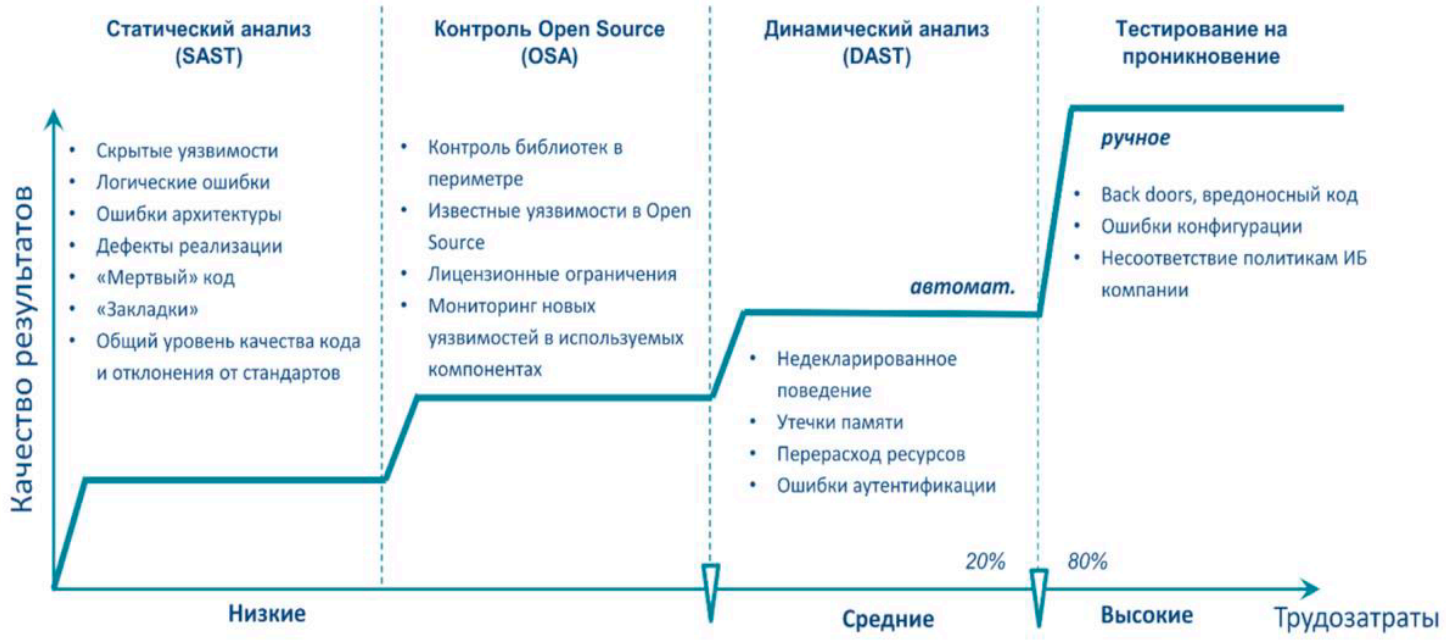

Рисунок 1 – shift-left подход

Дополнительный комментарий: далее в последующих кейсах приводятся пояснения в совокупном сочетании. Также требуется дополнительное сопроводительное пояснение к решениям кейсов. Пояснение описывают примеры подхода, так как они не конечны и необходима плоскость конкретики. Все решения описаны – как надо правильно, не исключая логику.

2. Какие вы видите риски в процессе управления изменениями информационных систем (от постановки задачи от бизнес-заказчика до установки модификации на продакшен) и какими мерами можно предотвратить и/или снизить эти риски?

Ответ: Выявление – оценка – планирование мероприятий по предотвращению – предусмотренные действия при наступлении – мониторинг. В процессном подходе использую методологию ориентированной на T-профиль команды по DASA DevOps. Применяю Agile-Lean концепции для минимизации потерь и максимизации конвейера потока ценности продукта на базе micro-services. Выстраиванию процессы в зависимости от проектов методики scrummerfall, scrum через transparency, freguent inspection, adaptation. Шаги: CASH - FLOW - COST - SECURITY - LEADTIME - QUALITY. Использую в работе метод Копнена-Трего, аналитику по событию Kaizen (принцип DMAIC) или Kaikaku (радикал) в зависимости от критериев срочности проекта и выходных метрик. Приоритизация осуществляю по KANO, либо MoSCoW. Оценка по RICE. Для более мелких фич используется доставка по JiT. Просчет работы в процессе спринта по закону Литтла. Основное взаимодействие с командой: Product Vision - Соглашение со стейкхолдерами - Impact Mapping - Product Roadmap to Value и из него вытекающее по процессу SCRUM - вплоть до ретроспективы и аналитики по принципу 5 reasons of why. Ключевое передается заказчику по DoD, в процессе работы для эффективности проектов через DoR (принцип INVEST). Стараюсь придерживаться фокуса на ценности продукта и поставки в спринтах максимально полезного продукта и сверху фич, иногда используется features toggle как триггеры в разработке с проблемными зонами и если необходимо переключение по поставке на не критичны ключах. Не использую gold plating или «марш смерти». Это эффективно по best practise и критерии оцениваются относительно ретроспективы, которая показывает результативности команды от спринта. Оценка проходит согласно с DT по категорированию product backlog в sprint backlog и расписанным ценностям INVEST. Также риски базируются на основании ожиданий и эмперического контроля. Риски вытекают от начальных этапов построения диалога между командами в формате эпика, для чего требуется детализация на уровне таксономии, придерживаясь бизнес-правил: политики, модели данных, принимание решение пользователем и владельцем исходя из возможных угроз, события, решения системы, жизненные циклы обьектов, вычисления, нормативные документы. Это все выливается в факты, ограничения, активаторы операций, выводы, вычисления.

Далее используется метод Кепнера-Крего через определение проблемы, описание, времени, размеров и затрагиваемых составных частей, установок возможных решений. После чего категорируется в формате классификации предоставленной информации: бизнес-требования, пользовательские требования, бизнес-правила, функциональные требования, атрибуты качества, требования к интерфейсам, ограничения, требования к данным, идеи решений. Впоследствии проходит аналитика по типу задач: описание принципа реализации, установление границ, поиск базовой платформы и альтернатив, разделение пользователей на группы, привлечение влиятельных пользователей. Процесс: роль – требование – обоснование. Все это выявляет и представляет из себя совокупные риски на каждом этапе следования, включая обратной связи, понятности дадачи, ее полноты и сложности и именно поэтому все вытекает в service relationship management (ITIL, ITSM, XLA/SLA, SMART) с принципами Lean Canvas. Виды потерь: человеческие, перепроизводство, ожидания, запасы, излишняя обработка, аналитический паралич, лишние движения. В последствии чего получается: kaizen event – value stream mapping – visual management – retrospective – daily standup – five times why. Занимался также планирование по Lean на базе Kanban: BUILD - MEASURE - LEARN - MVP по принципу Fail-Fast. Для команд кроссфункциональных - SCRUM. Ориентация принципа на конечном результате и ответственности за микросервис.

Риски ИТ-проекта:

- организационные:
-- недостаточная поддержка проекта со стороны высшего руководства
-- нарушение баланса интересов участников
-- недооценка сложности проекта
- человеческого фактора:
-- нежелание части персонала осваивать новые технологии
-- сложность освоения новых технологий
-- сопротивление руководителей, особенно среднего звена из опасений обесценивания
- технические риски:
-- жизненные циклы решений и платформа
-- неочевидные решения
-- отсутствие аналогов
-- ориентация на тупиковые технологии
-- неполнота и неточность исходной информации
- внешние риски:
-- недостаточное функционирование
-- несвоевременное финансирование
-- рыночная ситуация
-- нормативные органы

Использую для работы в коллективе: Lincolini, DMAIC, Kaizen, Обратная связь по бережливому стилю лидерства, Закон Конвея, Закон Литтла. Важна ориентированность на поток ценности продукта.

3. Если вы проверяете требования к парольной защите, установленные в корпоративном стандарте, какие минимально необходимые параметры вы ожидаете увидеть в этом стандарте и с какими присвоенными им значениями?

Ответ: длина пароля должна быть не менее 8 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.), пароль не должен включать в себя легко вычисляемые сочетания символов - имена, фамилии, номера телефонов и т.д., а также общепринятые сокращения, не должны использоваться автогенераторы, при смене пароля новое значение должно отличаться от предыдущего не менее чем в 8 позициях, личный пароль пользователь не имеет права сообщать никому, не должен быть закреплен на личных пк или записных книжек, кеширован внутри архитектуры active directory, должны быть словари по проверкам пароля и проверка по ним, есть ли коннекторы и как, где хранятся пароли, закешированы ли они и так далее.

4. Компания использует решения Oracle в качестве средства автоматизации бизнес-процессов. Решения установлены как на физических, так и на виртуальных машинах. Вам известно, что в Компании отсутствует

формализованный процесс управления ИТ активами (и hardware, и software). ИТ-директор сообщает вам о факте недолицензирования продуктов Oracle и затрудняется озвучить детали. Также вам известно, что в последние годы Oracle периодически заказывает аудиты на предмет соблюдения лицензионных требований у конкурентов рассматриваемой Компании в стране её присутствия. Опишите, пожалуйста:

a) Какие риски вы видите в этой ситуации?

b) Какие минимальные процедуры вы проведёте, чтобы количественно измерить риски, указанные вами выше? (для тех из них, где возможна количественная оценка)

c) Какие рекомендации предложите в данной ситуации?

Ответ:

а) штрафные санкции со стороны лицензионной политики; не возможность выхода на IPO и провал аудиторской проверки; эксплуатируемость уязвимостей не пропатченных версий, доступности в инфраструктуру, утечки инфомрации; размножение версий внутри инфраструктуры и на доменных контролерах; отсутствие механизмом контроля, взаимодействия между C-level и подчиненными; отсутствие владельцев ИР, их обслуживания, отказа в обслуживании и SLA/XLA; нарушение ДИ; не контролируемые доступы и отсутствие понимания архитектуры организации, информационных потоков, связей и контроля в ней.

б) построение карты архитектуры инфраструктуры, сетевые шары, сервера; идентификация пользователей; вид информация обрабатываемой на серверах, где крутится решение; версионность решения; интеграционные стыки с не пропатченными решениями; регламенты доступа к ИР; кто имеет доступ и кто ставил версии без лицензии; разбор инцидента и его фиксация.

в) внесение изменений в ОРД типа ПИБО, ДИ; открыть доменную учетку и проверить машины на которых стоят версии oracle через обновление по GPO и в ручном режиме по процессам на стороне терминала дерева процессов – отключить, если не критические узлы, в другом случае – перенести лицензионные версии и восполнить потерю; устранить не лицензионное ПО и обновить имеющиеся узлы; прогнать САВЗ на поиск установщиков и произвести жесткое удаление; проверить доступны на установку машины и учетные данные, которые их ставили, по правам пользования; вынести на help-desk разбор заявок на установку, обновление нелицензионного ПО; произвести внутренние проверки по правам пользователей, не идентифицированным аккаунтам и устранить процесс.

5. Компания собирается использовать облачное хранилище (вычисления, хранилища) для планируемой к внедрению информационной системы (далее – ИС). Вас привлекают в проектную команду по внедрению ИС и просят предложить меры для обеспечения безопасности данных (все составные части cia). Какие меры вы предложите как на техническом уровне, так и в части составления контракта с провайдером облака?

Ответ: если рассматривать полноценно цикл по Паркеровской гексаде – тогда в зависимости от платформы IaaS, либо PaaS, я могу сделать следующее предложение: для платформенного сервиса и инфраструктурного важно понимать расположение облака и правила сервиса, которое будет использоваться – его ограничения и политику, следовательно, по SWOT-анализу будет выдано лучшее решения для развертывания ИС. По мерам обеспечения комплексной безопасности, не касаясь AppSec в прямом его понимании, а в плоскости архитектуры – самое лучшее решение будет встроить в процесс DevSecOps Toolchain по (Рисунок 2).

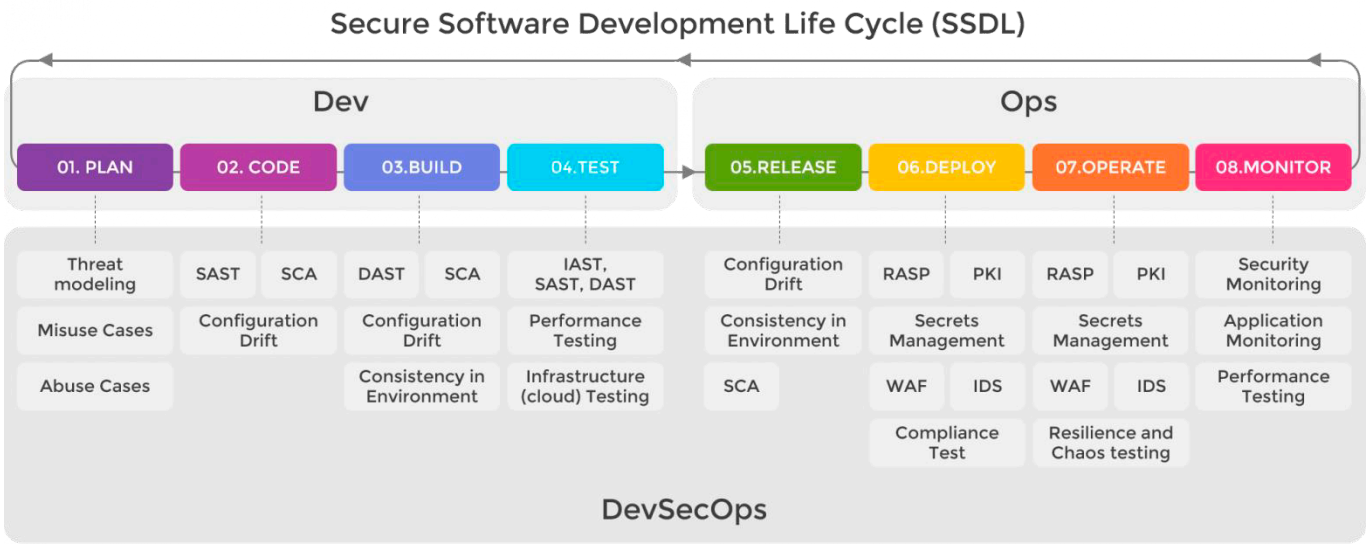

Рисунок 2 – DevSecOps Toolchain

С технической стороны также будет использоваться внутренняя структура организации процессов с использованием примера Amazon AWS: IAM AWS Authentication на permissions.cloud типа aws.permissions.cloud; RDS; Redis; Бастион; S3 Event Notifications + EventBridge; AWS Cloud Adoption Framework – использовать как playbook от и до, ECS-optimized AMI, Identity Federation for GitHub Actions on AWS; AWS Elastic Disaster Recovery; мультирегиональная репликация S3; AWS Secure Environment Accelerator; WAF к EKS; Security at the Edge; Ransomware Risk Management on AWS Using the NIST Cyber Security Framework, etc.

Далее приводится на (Рисунок 3) детали по рискам в облаке.

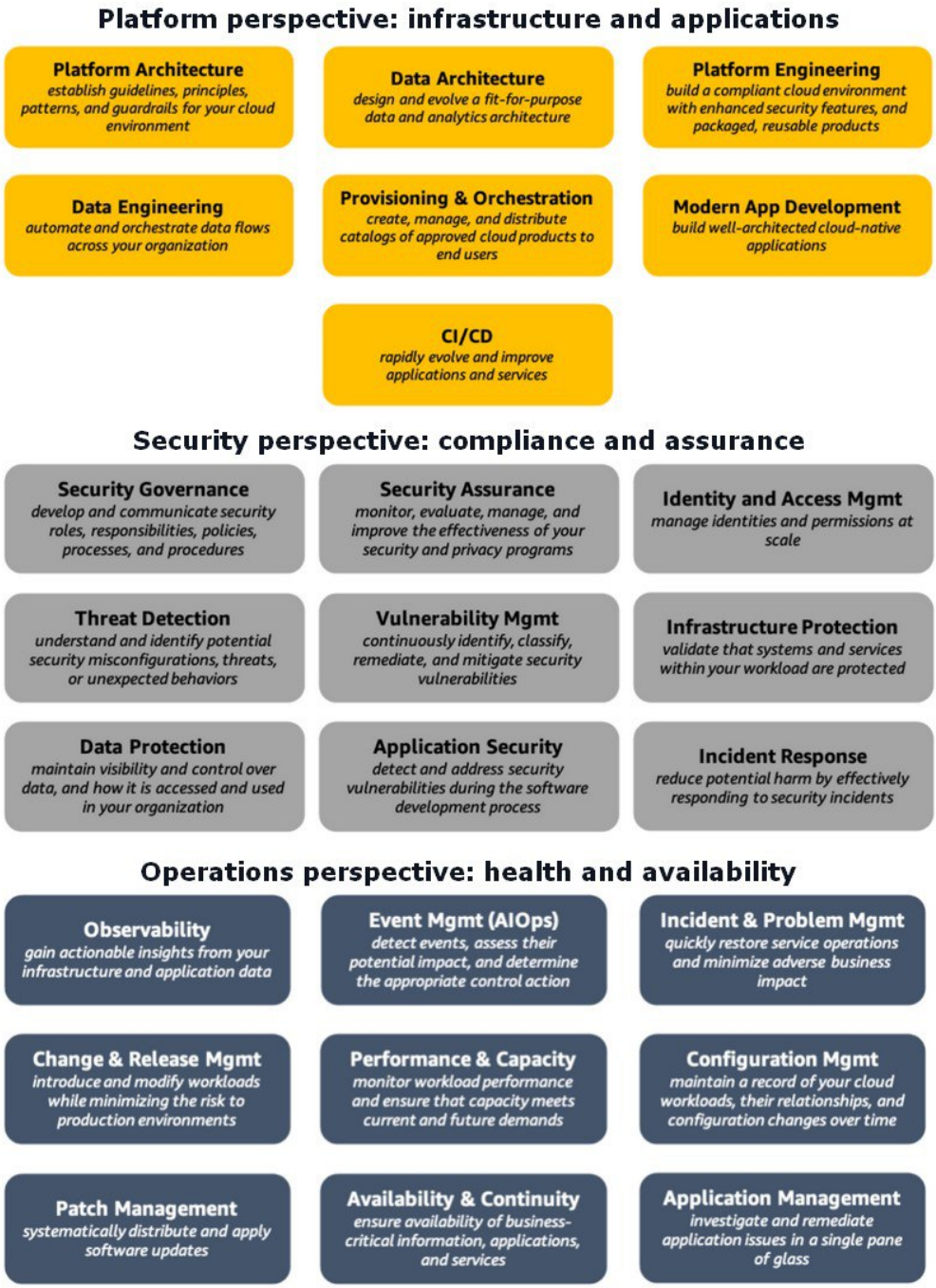

Рисунок 3 – риски перехода в облако

Насчет ОРД иметь место будет NDA с приложением конкретного списка-перечня обрабатываемой информации; доступности сервисов; обеспечения time-up для предотвращения потери данных их распределенное хранение и полный регламент сервисов; далее требуется проверка однозначности соглашения по портфелю услуг исходя из требований контракта, которые необходимы для развертывания ИС. Основное благоприятное решение для минимизации трат – это делегирование ответственности, если информация не критичная для организации и не требует особого контроля. В другом случае соглашения упираются в правила платформы как например выше по playbook.

6. Компания проводит ежегодное обновление своей программы непрерывности бизнеса. Координатор программы сталкивается со следующей проблемой: после распределения доступных ресурсов для резервирования трёх наиболее критичных ИС перед ним стоит задача по резервированию двух ИС следующего приоритета; ресурсов на обе ИС недостаточно. Бизнес-владельцы обеих ИС при совместной встрече с координатором программы утверждают, что резервирование их ИС критично важно для бизнеса. Кто в Компании должен принять решение о выборе ИС для финансирования её резервирования или о дополнительном финансировании программы?

(в рамках задачи можно пренебречь способами резервирования, достоверностью комментариев владельцев о важности ИС, а также точностью расчётов необходимого финансирования; в ответе интересует именно роль необходимого сотрудника)

Ответ: считаю уместным колаборацию между следующими стейкхолдерами по методу 6-3-5 в ролях – руководитель центра компетенций ИТ и инфраструктуры, CISO – определив наиболее критичные ИР и содержание данных. Ключевое решение принимается в формате резервирования данных на сьемные носители и выделение кластера данных из вне, то есть CISO предлагает бюджетодержателю факт достоверности обьемов хранения данных и отказа в обслуживании.

7. Компания использует терминальные сервера во внешнем сегменте сети для подключения к ним сотрудников при удалённой работе. Сотрудники имеют возможность подключиться к терминальному серверу по rdp с личных устройств. При подключении сотруднику необходимо ввести доменные логин и пароль. Какие риски вы видите в подобной конфигурации и какие меры предложите?

Ответ: риски НСД ; утечки информации; теневого копирования информации; отказа в обслуживании (если разработчик или доверенное лицо); терминалы требуется перезагружать и несохраненная информация может быть утеряна; возможность подключения к инфраструктуре с любых сторон; отсутствие Паркеровской гексады; нет идентификации пользователя; нет журналирования действий пользователя; свободный доступ к ИС внутри инфраструктуры и т.д. Решение классическое через использования выдачи корпоративного оборудования и его шеринга среди персонала, включая однозначной перепривязки через ТП при выдаче устройства в конечном виде; представить ноутбук как тонкий клиент и на уровне BIOS зашифровать паролем, где при не правильном вводе пароля – он превращается в нерабочее устройство; СДЗ (крайний случай на топ менеджменте ключевого направления, проще выдать арм внутри офиса); СЗИ от НСД типа SNS; DLP; IPS; самое главное отключить возможность rdp из вне и закрыть только на внутреннюю структуру при авторизации под учетной записью MS AD; Cisco AnyConnect и далее VMWare Horizen со сферой внутри инфраструктуры.

8. Вы (в роли внутреннего аудитора) обнаруживаете следующую ситуацию: при последнем запуске сканнера уязвимостей 20 дней назад была выявлена уязвимость с оценкой 8 по CVSS на почтовом сервере. Владелец почтового сервиса Компании – служба ИТ, так как сервис используется большинством сотрудников Компании и невозможно определить наиболее заинтересованное в сервисе бизнес-подразделение. Сотрудники службы ИБ прокомментировали, что их действия были следующие:

- Консультация со службой ИТ, которая сообщила о невозможности установки патча на сервер, так как его операционная система уже не поддерживается вендором;
- Принятие решения внутри службы ИБ о невозможности остановки сервиса ввиду потребностей бизнеса (почтовый сервер ежедневно обрабатывает в среднем 70000 писем) – ввиду этого было решено оставить ситуацию as is.

Какие рекомендации и в чей адрес вы адресуете в данном сценарии?

Ответ: отдел ИБ так как принял не верное решение и ИТ так как не смог провести сервисное обслуживнаие по ITIL, о том, что не была решена задача и собственнику путем эскалирования по организационно-штатной структуре организации будет выданы следующие рекомендации – если риск допустимый для организации и не несет критичных потерь по финансовой составляющей и его расследование много меньше, тогда лучше его принять, и сделать далее в мягком реджиме описанное далее. В другом случае и как вследствие первого варианта – поднять дупликат сервера, произвести обновления, реплицировать данные в мягком формате, подготовить дубликат всей операционной деятельности с актуальными обновлениями, в не рабочее время предупредить пользователей и далее произвести миграцию всей операционной деятельности через службу ТП. Адаптация сегментации MS Exchange.