По идее если мы уже работаем в крупном российском банке в 2019 году, то на мой взгляд, ИБ должна быть достаточно хорошо налажена. Поскольку задание у нас учебное и идея его в том, чтобы разобраться, как лучше повышать защищенность компании, то давайте немного скорректируем нашу легенду: пусть мы проснулись в должности CISO, ничего не помним, и нам Леночка из бухгалтерии кричит, что нужно срочно формировать бюджет на повышение защищенности компании на следующий год. Мы вообще не понимаем, что происходит, и идём в интернет для того, чтобы разобраться в ситуации.

Для начала ознакомимся со всеми предложенными вариантами:

1. ISO 27001

Стандарт ISO 27001 − это набор лучших **практик**, т.е. в их основе лежит полученная в реальной жизни отдача от внедрения тех или иных защитных технологий или мер. По мере поиска я наткнулся на отличную статью, описывающую сертификацию по упомянутому стандарту в России. Основная мысль в том, что нужно сначала разобраться с процессами в организации, а потом уже получать данный сертификат, потому что по ISO 27001 сертифицируется ПРОЦЕСС, а не компания и не система защиты. И часто бывает так, что внедрение формальное, только ради получения заветной бумажки. Мы в свою очередь хотим не просто сделать красивую обёртку, а реально принести пользу компании и заняться делом. Лучше было бы включить этот пункт в бюджет, когда мы действительно убедимся в том, что готовы к этой стандартизации.

2. PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) — стандарт безопасности данных индустрии платежных карт. Другими словами, это документация со списком критериев, которому должен удовлетворять сервис, если он как-то управляет такими вещами, как номер карты, срок её действия

и CVV-код. Читаю я, значит, про этот стандарт и понимаю, что мы – БАНК!!! Нам жизненно необходимо соответствовать данному стандарту, так как мы просто обязаны предоставить пользователям гарантии того, что их платежные данные находятся в безопасности. При невыполнении требований стандарта вступают санкции от платежных систем и банков эквайеров. Любое взаимодействие платежной системы с организациями, к ней подключенными, происходит через компанию принципала – те банки, эквайеры или эмитенты, которые непосредственно подключены к платежной системе. По правилам платежных систем еще до середины 2012 года было установлено, что ни одна организация, которая хранит, обрабатывает, а также влияет на безопасность карточных данных, не может не соответствовать требованиям PCI DSS. С того времени все компании уже должны соответствовать стандарту. В случае большого банка (больше 6 млн транзакций в год) необходим ежегодный QSA аудит и ежеквартальное ASV-сканирование, чтобы соответствовать PCI DSS level 1. Итак, проходить данную сертификацию необходимо каждый год, так что проведение аудита соответствия стандарту PCI DSS обязательно включаем в бюджет!

3. Red Team

Цель Red Team − проверить возможности организации по выявлению и предотвращению вторжения. В ходе редтиминга не производится поиск кучи уязвимостей, а лишь тех, что нужны для достижения цели. Цели обычно те же, что и при пентесте. В ходе редтиминга используются такие методы, как социальная инженерия (физическая и электронная), атаки на беспроводные сети, внешние активы и т.д. Такое тестирование — не для всех, а лишь для организаций со зрелым уровнем информационной безопасности. Такие организации обычно уже прошли пентесты, запатчили большинство уязвимостей и уже имеют опыт успешного противодействия тестам на проникновения. Считаю, что создание и содержание полноценной Red Team силами банка нецелесообразно, т.к. большая часть выполняемых задач

покрывается выполнением ISO и аудитов в рамках других работ. Возможно использование аутсорсной Read Team в рамках расширения бизнес-процессов (создание новых филиалов/отделений, дополнительная оценка критичных областей внутренних продуктов, не покрываемых иными аудитами).

4. Vulnerability Management

Управление уязвимостями отличается от простого сканирования сети, компьютеров, приложений, для обнаружения общих уязвимостей при помощи специальных программных средств. Сканирование является важным элементом управления уязвимостями, но управление уязвимостями включает в себя другие технологии, и рабочий процесс, необходимые для контроля и устранения уязвимостей. Основными целями VM являются:

• Выявление и исправления ошибок в программном обеспечении, которые влияют на безопасность, производительность и функциональность.

• Изменение конфигурации или улучшение функциональности программного обеспечения, чтобы сделать его менее восприимчивым к атаке.

• Эффективное управления рисками безопасности.

• Документирование состояния безопасности для аудита и соответствия законам, регуляторам, стандартам, политикам.

Комплексное, непрерывное управление уязвимостями сложно, если почти невозможно, реализовать ручным способом. Процесс управления уязвимостями включает в себя слишком много различных видов деятельности. Выполнение повторяющихся задач ручным способом, занимает чрезвычайно много времени и приводит к неэффективному использованию время ИТ персонала. По этой причине, организации стремятся автоматизировать и упростить, насколько это возможно, каждый элемент управления уязвимостями. Центр интернет-безопасности (CIS) рекомендует использовать средства управления уязвимости как базовое, поэтому однозначно включаем в бюджет. На самом деле данный пункт

должен быть выполнен в рамках ISO, т.к. этого требуют пункты A8.2.1, A.12.6, A.16.1.

5. СТО БР ИББС

Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (**СТО БР ИББС**) — комплекс документов Банка России, описывающий единый подход к построению системы обеспечения ИБ организаций банковской сферы с учётом требований российского законодательства. Документы носят рекомендательный характер, но согласно текущему закону исполнение требований стандарта обязательно только в том случае, если он уже принят. В противном случае можно его не исполнять. К примеру до выхода в 2018 году СТО для аутсорса, передача на аутсорс ИТ инфраструктуры без нарушения рекомендаций стандарта была невозможной. Более того, в стандарте есть требование на обязательное использование сертифицированного ФСТЭК оборудования, что не всегда возможно. Одно дело ─ выполнить некоторые положения стандарта для того, чтобы можно было поставить АРМ КБР и не нарушать другие ФЗ, а другое дело ─ соответствовать всем пунктам стандарта. Но если банк крупный, то он уже соответствует данному стандарту, поэтому нужно просто проводить аудит. Нашему банку важно соответствие не только требованиям признанного отраслевого стандарта, которым является СТО БР ИББС, но и законодательным требованиям, в том числе требованиям Федерального закона «О персональных данных». СТО БР ИББС содержит общие требования по обработке персональных данных и обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные. Приведение в соответствие с отраслевыми стандартами является важным шагом в повышении защищенности компании.

6. Проведение комплексного теста на проникновение.

Пентест заключается в выявлении максимального числа уязвимостей и ошибок конфигурации за отведённое время, а также в их эксплуатации для определения уровня риска. чаще всего это поиск известных незакрытых уязвимостей. Это достаточно важная часть на пути к повышению защищенности компании. проводить комплексную оценку защищенности, включающую проведение тестирования на проникновение рекомендуется и выявления известных уязвимостей компонентов АБС (п.9.5 РС БР ИББС-2.6-2014) рекомендуется еще на стадии приемки и ввода в действие. На стадии эксплуатации также необходимо выполнять периодическую оценку защищенности АБС и осуществлять мониторинг сообщений об уязвимостях АБС и реагирование на них (п.10.1 РС БР ИББС-2.6-2014). И, наконец, на стадии модернизации АБС рекомендуется проводить комплексную оценку защищенности в необходимом объеме (п.11.3 РС БР ИББС-2.6-2014).

Исходя из полученных знаний, можно сделать вывод о том, что если наша организация является крупным российским банком, то нам необходимо иметь очень высокий уровень защищенности компании и соответствовать необходимым стандартам.

Итак, подводя итоги, сделаем следующее заключение:

Для начала построим процесс управления уязвимостями, который в целом направит нас на дальнейшие действия. Затем приведем все в соответствие с отраслевыми стандартами, выполнив необходимые рекомендации, в том числе комплексное тестирование на проникновение. На этом этапе мы в теории можем организовать команду Red Team и готовиться к подтверждению соответствия стандарту PCI DSS (нам нужно его не получить, а подтвердить, так как если мы уже являемся крупным российским банком, то мы точно его получали и даже возможно неоднократно подтверждали). Что касается построения системы управления информационной безопасностью в соответствии с лучшими практиками ISO

27001, − это достаточно спорный вопрос, но можно порассуждать при ответе на него с точки зрения банковской сферы.

Сертификация по ISO-27001 является достаточно трудоёмким и непростым процессом, а потому нужно представлять себе, какие преимущества она может дать организации, которая на неё решится. На сайтах и в рекламных брошюрах тех консалтеров, которые оказывают услуги по сертификации, можно найти красочное перечисление всего того, что должна дать сертификация отважившейся на неё компании. Конечно, далеко не все из радужных обещаний оказываются воплощенными на практике, но, тем не менее, ряд плюсов сертификация компании всё-таки даёт.

Первое и, зачастую, наиболее весомое преимущество – имиджевое. Пройдя сертификацию, банк может повысить привлекательность в глазах корпоративных клиентов и партнеров, которые внимательно относятся к вопросам обеспечения информационной безопасности.

Впрочем, как говорится в рекламе одного достаточно известного напитка, имидж – ничто. Особенно в тех случаях, когда с безопасностью действительно есть заметные невооруженным глазом проблемы. Поэтому второе по счету (а по важности, пожалуй, первое) преимущество прохождения сертификации по ISO-27001 – это улучшение ситуации с обеспечением информационной безопасности в организации. К сожалению, зачастую руководители не понимают того факта, что в перспективе это означает существенную экономию благодаря отсутствию ущерба от инцидентов в сфере информационной безопасности. Конечно, банковской сфере в этом плане, можно сказать, повезло больше, чем, например, промышленности, но и в ней часто можно встретить непонимание руководителями далеко идущих последствий обеспечения или необеспечения информационной безопасности в их компаниях.

Третьим наиболее значимым преимуществом внедрения ISO-27001 является повышение прозрачности работы всех отделов для высшего руководства компании. Это касается и отдела информационной безопасности, деятельность которого для многих руководителей сродни какому-то непонятному магическому ритуалу.

Конечно, на этих трёх пунктах список тех плюсов, которые может получить организация, пройдя сертификацию по ISO-27001, не заканчивается. Для каждого банка, страховой компании, лизинговой компании или другой финансовой организации эти преимущества могут быть своими, в зависимости от текущего положения дел в обеспечении информационной безопасности и от того, какие задачи ставит перед собой отдел информационной безопасности при прохождении сертификации.

Принципиальным при прохождении сертификации является именно вопрос постановки цели: для чего требуется прохождение сертификации – для соответствия формальным требованиям, записанным в стандарте, или для реального повышения уровня защищенности от информационных угроз? Понятно, что при выполнении «от корки до корки» всех требований стандарта получится повысить и уровень защищенности, но цена за это может оказаться достаточно высокой. Поэтому необходимо тщательно проанализировать стандарт и то, насколько сложно его будет применить при текущей организации бизнес-процессов в вашей компании. Вполне может оказаться, что нет смысла использовать весь стандарт целиком – возможно, рациональнее будет постараться применить в ваших условиях только отдельные его части, либо же вовсе нанять опытного и грамотного «безопасника», который сможет реорганизовать работу отдела информационной безопасности «не по бумажке»

Также на мой взгляд в пункты стандартов необходимо добавить как минимум SWIFT Cert, т.к. без SWIFT очень сложно проводить

международные транзакции. Если банк российский, то скорее всего он захочет обслуживать бюджетников, а для этого ему нужно пройти стандартизацию для платежной системы МИР (опросник SAQ D-MIR). Кроме этого, необходимо ещё создать SOC первой линии, а более сложные задачи отдать на аутсорс.

Red Team, Пентест, стандартизацию по ISO и PCI DSS нужно зааутсорсить у какого-то одного контрагента, что позволит существенно сэкономить на внедрении стандарта и последующих аудитах, в том числе и финансовых, где придётся выполнять ITGC, а у нас на руках будет заключение о том, что всё хорошо. Данные меры позволят:

1) Сэкономить на сотрудниках;

2) Упростить визиты проверяющих органов, так как на руках будут не гипотетические заключения наших специалистов, а бумага из аудиторской компании, что решит огромное количество вопросов;

3) Уровень квалификации сотрудников в компаниях по ИБ обычно выше, чем в банках, т.е. при правильном выборе аутсорс-контрагента, качество тоже должно подрасти;

4) Престиж. Если на сайте написано, что аудит проведен зарекомендовавшей себя ранее компанией, а не собственными силами, то это круче + по многим стандартам всё равно нужен внешний аудит;

5) Если вдруг кто-то дистанционно украдет активы, то контрагент будет искать негодяев и возвращать деньги как можно скорее, ведь они дорожат своим именем.

Можно еще много рассуждать на эту тему, но думаю, что для начала будет достаточно ☺

Спасибо за интересное задание!