МИНИСТЕРСТВО ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ

АЗЕРБАЙДЖАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

На правах рукописи

АББАСЗАДЕ РАХМАН НАТИГ оглы

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

НА ТЕМУ:

Исследование информационной безопасности экономических систем

Наименование и шифр специальности: 060632 Инженерия информационных технологий и систем

Наименование специализации: Информационная защита и безопасность

Научный руководитель: **доцент Х.М.Байрамов**
Руководитель магистерской программы: **акад. Аббасов А.М.**
Заведующий кафедрой: **акад. Аббасов А.М.**

БАКУ – 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы. Защита киберпространства и электронных коммуникаций стала правительственным и отраслевым приоритетом во всем мире. Растущее значение информационных и коммуникационных технологий в важнейших функциях экономики усилило необходимость принятия мер по предотвращению и защите во всех секторах, в том числе в финансовом секторе.

Это исследование было направлено на понимание и сравнение обязательств, касающихся информационной безопасности, в финансовом секторе в большинстве стран чтобы сравнить их с отраслевыми перспективами, и наметить четкое видение важных приоритетов на будущее.

Цель исследования. Целью данного исследования является оценка современных приложений безопасности для банков и учетных информационных систем. Для достижения этой цели был проведен опрос с использованием изначально созданных опросников.

Результаты исследования показывают, что банки используют современные приложения безопасности, а также показывает, что банки испытывают недостаток в информационных системах учета.

Основная рекомендация для этого исследования - увеличить силу обучения по всем направлениям в информационных системах учета, чтобы минимизировать возможные угрозы.

Предмет исследования. Объектом исследования в основном стали экономические и финансовые организации не зависимо от страны, и автоматизированные системы информационной безопасности, требуемые для защиты своих организаций от несанкционированного доступа как извне, так и кражи конфиденциальных данных изнутри компании. Также пути для обеспечения максимальной защиты конфиденциальных данных для выявления максимально эффективных методов при минимальных расходах времени и финансовых усилий

Теоретическая основа диссертации. При написании данной диссертацией автором были использованы работы широкого круга иностранных и отечественных ученых по вопросам как общего характера, так и непосредственно относящимся к теме диссертации.

Теоретическую основу данного исследования составляют работы зарубежных и отечественных авторов, а также документы международного характера, которые относятся к рассматриваемым проблемам. В ходе работы над диссертацией автором использовались труды таких ученых как: В.Н. Ясенев, С.А. Нестеров и др.

Методологической базой исследования являются последние работы ученых как зарубежных, так и отечественных по данной проблеме об обеспечении необходимой безопасности, также исследования научных групп и университетов в данной сфере.

Комплексный и системных подход для обеспечения поставленной задачи который был применен в данных исследованиях и составил для него методологическую базу.

Научная новизна. Научная новизна исследования заключается в комплексном подходе к проблемам, присущим современному состоянию информационных технологий по безопасности.

Ряд вопросов, исследованных в этой диссертации, носят характер научной новизны. К их числу относятся: исследование новейших технологий защиты информационных систем, а также системы анализа, тестирования и выявления ошибок системы с использованием последнего программного обеспечения и также выявлены различия между ними.

Теоретическая и практическая ценность исследования состоит из основных рекомендаций, положений и заключений для организации устранения проблем безопасности в экономических системах. Здесь заключается способы и методы решения проблем информационной безопасности различными способами и в зависимости от деятельности учреждения в целом.

ГЛАВА I. ВИДЫ ИНФОРМАЦИОННЫХ УГРОЗ И ИХ ПОНЯТИЯ

1.1. Основные понятия

Информационная безопасность — это концепция, которая становится все более запутанной во многих аспектах нашего общества, в основном в результате нашего почти повсеместного внедрения компьютерных технологий. В нашей повседневной жизни многие из нас работают с компьютерами для наших работодателей, играют на компьютерах дома, ходят в школу онлайн, покупают товары у торговцев через Интернет, приносят наши ноутбуки в кафе и проверяют нашу электронную почту, используют смартфоны для проверки баланса нашего банка, отслеживания наших упражнений с датчиками в обуви и так далее, до бесконечности.

Хотя эта технология позволяет нам быть более продуктивной и позволяет получать доступ к множеству информации одним щелчком мыши, она также сопряжена с множеством проблем безопасности. Если информация о системах, используемых нашими работодателями или нашими банками, становится уязвимой для злоумышленника, последствия могут быть действительно ужасными. Мы можем внезапно оказаться лишенными средств, так как содержимое нашего банковского счета передается в банк в другой стране посреди ночи. Наша компания может потерять миллионы долларов, подвергнуться судебному преследованию и нанести ущерб своей репутации из-за проблемы конфигурации системы, позволяющей злоумышленнику получить доступ к базе данных, содержащей информацию, позволяющую установить личность (PII), или конфиденциальную информацию. Мы видим, что такие примеры появляются в СМИ с тревожной регулярностью.

Если мы оглянемся на 30 лет назад, таких проблем, связанных с компьютерными системами, почти не было, в основном из-за низкого уровня внедрения технологий. Если мы сможем получить хорошее представление об основах информационной безопасности, мы сможем справиться с изменениями по мере их появления.

Мы можем столкнуться с атаками с самых разных подходов и векторов. Когда мы смотрим на то, что именно составляет атаку, мы можем разбить ее в зависимости от типа атаки, которую она представляет, риска, который представляет атака, и средств управления, которые мы могли бы использовать, чтобы смягчить ее.

Значение термина компьютерная безопасность развилось в последние годы. Перед проблемой о безопасности данных стали широко освещаться в средствах массовой информации, большинство людей считают, что компьютерная безопасность сосредоточена на физической машине. Традиционно, компьютерные средства были физически защищены по трем причинам:

• Для предотвращения кражи или повреждения оборудования

• Для предотвращения кражи или повреждения информации

• Для предотвращения срыва обслуживания

Компьютерная безопасность — это безопасность, применяемая к вычислительным устройствам, таким как компьютеры и смартфоны, а также компьютерные сети, такие как частные и публичные сети, включая весь интернет. Поле охватывает все процессы и механизмы какое цифровое оборудование, информация и услуги защищены от непреднамеренного или несанкционированного доступа, изменения или уничтожения, и приобретают все большее значение в соответствии с растущей зависимостью от компьютерных систем большинства обществ во всем мире. Включает в себя физическую безопасность для предотвращения кражи оборудования и информационная безопасность для защиты данных на этом оборудование. Иногда его называют кибербезопасность или безопасность ИТ, хотя эти термины как правило, не относятся к физической безопасности (замки и тому подобное).

Некоторые важные термины, используемые в компьютерной

безопасности[14]:

Уязвимость

Уязвимость — это слабость, которая позволяет злоумышленнику уменьшить объем информации, поступающей от системы.

Уязвимость — это пересечение трех элементов: уязвимости системы или недостатка, доступ злоумышленника к недостатку и способность атакующего использовать недостаток. Для использования уязвимости злоумышленник должен иметь хотя бы один применимый инструмент или метод, который может подключиться к системной слабости. В этом случае уязвимость также называется началом атаки.

Управление уязвимостями — это циклическая практика выявления, классификации, исправления, и устранение уязвимостей. Эта практика обычно относится к уязвимостям программного обеспечения в вычислительные системы.

Бэкдор

Бэкдор в компьютерной системе, это метод обхода обычной аутентификации, обеспечение безопасности удаленного доступа к компьютеру, получение доступа к незашифрованному тексту и т. д. при попытке остаться незамеченным.

Бэкдор может принимать форму установленной программы (например, Back Orifice) или может быть модификация существующего программного или аппаратного устройства. Это может также подделать информацию о использование диска и памяти.

Атака отказа в обслуживании

В отличие от других типов атак, атаки типа отказ в обслуживании не используются для получения несанкционированного доступа или управление системой. Вместо этого они разработаны, чтобы сделать его непригодным для

использования. Злоумышленники могут отрицать обслуживание отдельных жертв, например, путем преднамеренного ввода неправильного пароля. Это может привести к блокировке учетной записи жертвы или к перегрузке возможности машины или сети и блокировать всех пользователей одновременно.

Атаки с прямым доступом

Несанкционированный пользователь, получивший физический доступ к компьютеру (или его части), может выполнять множество функций, установка различных типов устройств, чтобы поставить под угрозу безопасность, в том числе операционные модификации системы, программные черви, клавиатурные шпионы и скрытые устройства прослушивания.

Злоумышленник также может легко загружать большие объемы данных на носитель экземпляр CD-R / DVD-R, кассета; или портативные устройства, такие как ключевые диски, цифровые камеры или цифровые аудиоплееры. Другая распространенная техника — это загрузка операционной системы. Она содержится на компакт-диске или другом загрузочном носителе и считывает данные с жесткого диска (дисков) сюда. Единственный способ победить это зашифровать носитель и сохранить ключ отдельно от системы. Атаки с прямым доступом - единственный тип угроз к автономным компьютерам (никогда не подключающимся к Интернету), в большинстве случаев.

Подслушивание

Подслушивание — это тайное прослушивание частного разговора, обычно между хостами в сети. Например, такие программы, как Carnivore и NarusInsight, использовались ФБР и АНБ для прослушивания систем провайдеров интернет-услуг.

Подделка

Подмена идентификатора пользователя описывает ситуацию, в которой один человек или программа успешно маскируется под очередную

фальсификацию данных и тем самым получает незаконное преимущество.

Фальсификация

Подделка описывает преднамеренную модификацию продуктов таким образом, чтобы они вредно для потребителя.

Отречение

Отказ описывает ситуацию, когда подлинность подписи оспаривается.

Раскрытие информации

Раскрытие информации (нарушение конфиденциальности или утечка данных) описывает ситуацию, когда информация, считаемая безопасным, выпускается в ненадежной среде.

Возвышение привилегий

Повышение привилегий описывает ситуацию, когда человек или программа хотят получить повышенные привилегии или доступ к ресурсам, которые обычно ему / ей ограничены.

Бреши

Эксплойт — это часть программного обеспечения, кусок данных или последовательность команд, которая принимает преимущество программного обеспечения ошибка или сбой для того, чтобы вызвать непреднамеренные или непредвиденные поведение на компьютерном программном обеспечении, оборудовании или чем-то электронном (обычно компьютеризированный). Это часто включает в себя такие вещи, как получение контроля над компьютерной системой или разрешением повышения привилегий или атакой отказа в обслуживании. Термин эксплуатировать в целом относится к небольшим программам, разработанным для использования недостатков программного обеспечения, которые были обнаруженный, удаленный или локальный. Код из эксплойта часто используется повторно в троянских конях и компьютерных вирусах.

Косвенные атаки

Косвенная атака — это атака стороннего компьютера. Используется чужой компьютер, чтобы начать атаку, становится гораздо сложнее отследить фактического злоумышленника.

Также были случаи, когда злоумышленники использовали общедоступные системы анонимизации, такой как система маршрутизатора tor onion.

Компьютерное преступление: компьютерное преступление относится к любому преступлению, которое включает компьютер и сеть[20].

Рисунок 1. Структура понятия Информационная безопасность.

Сегодня большинству организаций нужны информационные системы для выживания и процветания. Информация стала ценным активом для

современных организаций. Поэтому современные организации должны серьезно относиться к защите своих информационных ресурсов. Эта защита информационных ресурсов, также известная как информационная безопасность, состоит из множества процессов. Некоторые из этих процессов, в значительной степени, зависят от поведения человека в сотрудничестве. Сотрудники, умышленно или по неосторожности, часто из-за недостатка знаний, представляют наибольшую угрозу информационной безопасности. Без адекватного уровня взаимодействия и знаний пользователей многие методы безопасности могут быть неправильно использованы или неверно истолкованы пользователями. Это может привести к тому, что даже адекватная мера безопасности станет неадекватной. Таким образом, стратегия информационной безопасности организации должна комплексно учитывать этот человеческий фактор. Важно отметить, что существует два аспекта этого человеческого фактора в информационной безопасности, а именно знания, сотрудничество и поведение. Эти измерения в значительной степени взаимосвязаны друг с другом. Организации не могут защитить целостность, конфиденциальность и доступность информации в сегодняшней среде сетевых систем с высокой степенью интеграции, не гарантируя, что каждый участвующий человек разделяет это видение безопасности организации, понимает свои роли и обязанности, и имеет соответствующую подготовку для их выполнения. Таким образом, чтобы помочь в обеспечении информационной безопасности, отдельным пользователям необходимы знания относительно их конкретной роли в процессе обеспечения безопасности. Эти знания могут быть предоставлены в рамках образовательных, учебных и информационных кампаний. Как только эти пользователи получают достаточные знания об их ролях в процессе обеспечения безопасности, все еще нет гарантии, что они будут придерживаться своих необходимых ролей безопасности. Возможно, что пользователи правильно понимают свои роли, но по-прежнему не придерживаются политики безопасности, потому что это противоречит их

убеждениям и ценностям. Поэтому необходимо также обеспечить правильное отношение пользователей и, следовательно, желаемое поведение к информационной безопасности. Чтобы обеспечить желаемое поведение пользователя, необходимо развивать организационную субкультуру информационной безопасности. Такая культура должна поддерживать все виды деловой активности, поскольку информационная безопасность становится естественным аспектом повседневной деятельности каждого сотрудника. Образование сотрудников играет очень важную роль в формировании такой культуры. Крайне важно, чтобы люди были образованы, чтобы хотеть быть более защищенными в своей повседневной работе. Такое изменение отношения имеет первостепенное значение, потому что изменение отношения автоматически приводит к последующему поведенческому изменению. Посредством создания культуры информационной безопасности сотрудники могут стать активом безопасности, а не подвергаться риску. Многие недавние исследования показали, что создание культуры информационной безопасности в организации действительно необходимо для эффективной информации. Однако такая культура должна поддерживаться адекватными знаниями в отношении информационной. Без достаточных знаний пользователи, которые хотят вести себя безопасно, могут по-прежнему неправильно применять контроль безопасности. И наоборот, пользователь, который обладает достаточными знаниями, но считает, что безопасное поведение не является необходимым в его ее конкретной роли, может вести себя небезопасно. Из-за этой взаимозависимости между измерением знаний человеческого фактора в информационной безопасности и поведенческим измерением было бы полезно иметь дело с этими измерениями целостным образом. Таким образом, имело бы смысл иметь единую концептуальную основу, которую можно использовать для обоснования как знаний, так и поведенческих аспектов этого человеческого фактора в информационной безопасности. При изучении этого адаптированного определения важно понять, что знания и базовые

образовательные программы, необходимые для передачи таких знаний, часто рассматриваются как часть корпоративного культура. Целью здесь не является оспаривание этой точки зрения. Фактически, здесь поддерживается мнение, что знания и образование всегда будут играть роль в обеспечении определенных моделей поведения. Тем не менее, делается попытка подчеркнуть тот факт, что измерение знаний имеет особое значение в культуре информационной безопасности, и что знания в области безопасности играют весьма специфическую стимулирующую роль в информационной безопасности. Дополнительное знание измерение, которое будет представлено, представляет знания, необходимые для эффективной реализации или использования мер безопасности, если можно принять желаемое отношение. Знания, которые формируют основную часть любой корпоративной культуры, все еще предполагается оставить. В этом отношении культура информационной безопасности считается такой же, как нормальная корпоративная культура[18].

Информационная безопасность определяется как защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения. По сути, это означает, что мы хотим защитить наши данные (где бы они ни были) и системные ресурсы от тех, кто попытается использовать их не по назначению. В общем смысле безопасность означает защиту наших активов. Это может означать защиту их от атак злоумышленников, проникших в наши сети, вирусов / червей, стихийных бедствий, неблагоприятных условий окружающей среды, сбоев электропитания, кражи или вандализма или других нежелательных состояний. В конечном итоге мы попытаемся обезопасить себя от наиболее вероятных форм нападения, насколько это возможно, исходя из нашей окружающей среды. Когда мы смотрим на то, что именно мы защищаем, мы можем иметь широкий спектр потенциальных активов. Мы можем рассмотреть физические элементы, которые мы можем захотеть обезопасить, например, те, которые имеют внутреннюю ценность (например, золотые слитки) или те,

которые имеют ценность для нашего бизнеса (например, компьютерное оборудование). У нас также могут быть предметы такие как программное обеспечение, исходный код или данные. В сегодняшней вычислительной среде мы, вероятно, обнаружим, что наши логические активы по крайней мере так же ценны как наши физические активы. Кроме того, мы также должны защищать людей, которые участвуют в нашей деятельности. Люди - наш самый ценный актив, так как мы не можем вести бизнес без них. Мы дублируем наши физические и логические активы и сохраняем их резервные копии в других местах на случай возникновения катастрофы, но без квалифицированных людей, чтобы работать и поддерживать нашу среду, мы быстро потерпим неудачу. В наших усилиях по защите наших активов мы также должны учитывать последствия безопасности, которую мы выбираем для реализации. Есть известная цитата, которая гласит: Единственная действительно безопасная система — это система, которая выключена, отлита в бетонном блоке и запечатана в свинцовой комнате с вооруженной охраной - и даже тогда у меня есть сомнения. Хотя мы, конечно, можем сказать, что система в таком состоянии может считаться достаточно безопасной, она, безусловно, не пригодна для использования или продуктивна. Когда мы повышаем уровень безопасности, мы обычно снижаем уровень производительности. С системой, упомянутой в нашей цитате, уровень безопасности был бы очень высоким, но уровень производительности был бы очень близок к нулю. Цель плана обеспечения безопасности - найти баланс между защитой, удобство использования и стоимостью. Кроме того, при защите актива, системы или среды мы также должны учитывать отношение уровня безопасности к стоимости защищаемого элемента. Мы можем, если мы хотим учесть снижение производительности, очень высокий уровень безопасности для каждого актива, за который мы несем ответственность. Мы можем построить объект стоимостью в миллиард долларов, окруженный забором из колючей проволоки и патрулируемым вооруженными охранниками и злобными бойцами, и

аккуратно поместить наш актив в герметически закрытое хранилище внутри, так что рецепт шоколадного печенья мамы никто никогда не повредит, но это не имеет особого смысла. Однако в некоторых средах таких мер безопасности может быть недостаточно. В любой среде, где мы планируем повышенный уровень безопасности, мы также должны учитывать стоимость замены наших активов в случае их потери и обеспечить разумный уровень защиты их стоимости. Стоимость безопасности, которую мы устанавливаем, никогда не должна превышать ценность того, что она защищает. Когда мы в безопасности? Определение точной точки, в которой мы можем считаться безопасными, представляет собой нечто вроде вызов. Мы в безопасности, если наши системы исправлены? Мы в безопасности, если мы используем надежные пароли? Мы в безопасности, если мы полностью отключены от Интернета? С определенной точки зрения, на все эти вопросы можно ответить нет, поэтому реальный вопрос заключается в том, достаточно ли мы в безопасности. Даже если наши системы будут исправлены должным образом, всегда будут новые атаки, к которым мы уязвимы. Когда используются надежные пароли, будут другие проспекты, которые злоумышленник может использовать. Когда мы отключены от Интернета, наши системы могут быть физически доступны или украдены. Короче говоря, очень трудно определить, когда мы действительно в безопасности. Мы можем, однако, перевернуть вопрос. Определить, когда мы небезопасны, гораздо проще, и мы можем быстро перечислить ряд элементов, которые приведут нас в это состояние:

• Не исправление наших систем или недостаточно быстрое исправление

• Использование слабых паролей, таких как пароль или 12345678

• Загрузка зараженных программ из Интернета.

• Открытие опасных вложений электронной почты от неизвестных отправителей

• Использование беспроводных сетей без шифрования, которое может контролировать любой.

Мы могли бы долгое время дополнять этот список. Хорошая вещь заключается в том, что, как только мы сможем указать на области в среде, которые могут сделать ее небезопасной, мы сможем предпринять шаги для смягчения этих проблем. Эта проблема равна сокращению чего-либо пополам снова и снова; всегда будет оставаться небольшая часть, чтобы снова разрезать.

Хотя мы можем никогда не достичь состояния, которое мы можем окончательно назвать безопасным, но мы можем предпринять шаги в правильном направлении.

Соответствие требованиям является ключевым аспектом любой программы безопасности и должно координироваться во всей организации. Нормы права, определяющие стандарты безопасности, довольно сильно различаются в зависимости от отрасли и от страны к стране. Организации, которые работают по всему миру, очень распространены в настоящее время, и мы должны позаботиться о том, чтобы мы не нарушали такие законы в ходе проведения.

Некоторые законодательные или нормативные акты пытаются определить, что является безопасным, или, по крайней мере, некоторые из шагов, которые мы должны предпринять, чтобы быть достаточно безопасными. У нас есть стандарт безопасности данных индустрии платежных карт (PCI DSS) для компаний, которые обрабатывают платежи по кредитным картам. Закон о мобильности и подотчетности медицинского страхования (HIPAA) 1996 года для организаций, занимающихся медицинским обслуживанием и записями пациентов. Федеральный закон об управлении информационной безопасностью (FISMA), определяющий стандарты безопасности для многих федеральных агентств во многих странах. Являются ли эти стандарты эффективными или нет, является предметом большого обсуждения, но соблюдение стандартов

безопасности, определенных для отрасли, в которой мы работаем, обычно считается целесообразным, если не обязательным.

Три основных понятия в информационной безопасности - это конфиденциальность, целостность и доступность, обычно известные как триада конфиденциальности, целостности и доступности (CIA), как показано на диаграмме 1. Триада ЦДК дает нам модель, с помощью которой мы можем думать и обсуждать концепции безопасности, и, как правило, очень сосредоточены на безопасность, поскольку она относится к данным.

Учитывая элементы триады, мы можем начать обсуждать вопросы безопасности очень специфическим образом. В качестве примера мы можем посмотреть на поставку лент с резервными копиями, на которых хранится

Диаграмма 1. Триада ЦДК.

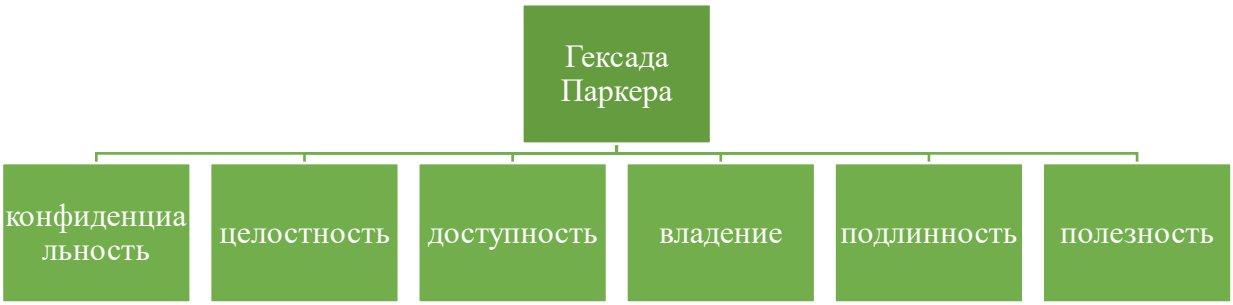
единственная существующая, но незашифрованная копия некоторых наших конфиденциальных данных. Если мы потеряем груз в пути, у нас возникнет проблема безопасности. С точки зрения конфиденциальности, мы, вероятно, столкнемся с проблемой, поскольку наши файлы не были зашифрованы. С точки зрения целостности, предполагая, что мы смогли восстановить ленты, у нас снова возникла проблема из-за отсутствия шифрования, используемого в

наших файлах. Если мы восстановим ленты и незашифрованные файлы были изменены, это не было бы сразу для нас очевидным. Что касается доступности, у нас есть проблема, ленты не будут восстановлены, так как у нас нет резервной копии файлов.

Хотя мы можем описать ситуацию в этом примере с относительной точностью, используя триаду ЦДК, мы можем обнаружить, что модель является более строгой, чем то, что нам нужно для описания всей ситуации. Существует альтернативная модель, которая несколько шире.

Паркеровская гексада, названная в честь Донна Паркера и представленная в его книге Борьба с компьютерным преступлением, дает нам несколько более сложный вариант классической триады ЦДК. Там, где триада ЦДК состоит из конфиденциальности, целостности и доступности, гексада Паркера состоит из этих трех принципов, а также владения или контроля, аутентичности и полезности, всего шесть принципов, как показано на диаграмме 2.

Диаграмма 2. Гексада Паркера.



Хотя некоторые считают его более полной моделью, гексада Паркера не так известна, как триада ЦДК. Если мы решим использовать эту модель при обсуждении ситуации с безопасностью, мы должны быть готовы объяснить как разницу, так и преимущества.

Как мы уже упоминали, гексада Паркера включает в себя три принципа триады ЦДК с теми же определениями, которые мы только что обсуждали. Существует некоторая разница в том, как Паркер описывает целостность, так

как он не учитывает санкционированное, но неверное изменение данных и вместо этого фокусируется на состоянии самих данных в смысле полноты.

Владение или контроль относится к физическому расположению носителя, на котором хранятся данные. Это позволяет нам, без привлечения других факторов, таких как доступность, обсуждать нашу потерю данных на физическом носителе. В нашей утерянной партии резервных лент предположим, что некоторые из них были зашифрованы, а некоторые - нет. Принцип владения позволил бы нам более точно описать масштаб инцидента; зашифрованные ленты в партии — это проблема владения, но не проблема конфиденциальности, а незашифрованные ленты - проблема в обоих случаях. Это очень важно в современной среде, где данные могут храниться на нескольких устройствах, и их может быть много.

1.2. Безопасность операционных систем

Когда мы стремимся защитить наши данные, процессы и приложения от согласованных атак, одной из самых больших областей, в которых мы обнаруживаем недостатки, является операционная система, на которой размещены все эти компоненты (будь то компьютер, маршрутизатор или смартфон). Если мы не позаботимся о защите наших операционных систем, у нас действительно не будет оснований для того, чтобы занять достаточно сильную позицию безопасности. Есть несколько способов, с помощью которых мы можем смягчить различные угрозы и уязвимости, с которыми мы можем столкнуться с точки зрения операционной системы. Одна из самых простых категорий, которую мы можем указать, — это усиление операционной системы. Мы можем использовать эту технику, когда настраиваем хосты, которые могут столкнуться с враждебным действием, чтобы уменьшить количество открытых портов, через которые злоумышленник может в конечном итоге добраться до нас. Мы также можем добавлять инструменты и приложения в нашу операционную систему, предназначенные для борьбы с некоторыми методами, которые злоумышленники могут использовать против нас. Наиболее

распространенным и очевидным из них является использование инструментов защиты от вредоносных программ, которые защищают нас от широкого спектра вредоносного кода, которому может подвергаться наша система, особенно если она обращена к Интернету.

В том же общем классе программного обеспечения мы также можем обратиться к программным брандмауэрам и системам обнаружения вторжений (HIDS) на уровне хоста, чтобы блокировать нежелательный трафик и предупреждать нас, когда нежелательный сетевой трафик поступает в наши системы или исходит из них. Кроме того, мы можем использовать большое количество доступных инструментов безопасности, чтобы помочь нам обнаружить потенциально уязвимые области на наших хостах. Мы могли бы использовать такие инструменты для поиска сервисов, которые мы не обнаружили во время наших усилий по усилению защиты, для определения сетевых сервисов, которые, как известно, содержат уязвимости, для проверки актуальности наших исправлений и для общей проверки аудита наших систем. Благодаря объединению всех этих усилий, чтобы еще раз вернуться к концепции глубокой защиты, мы можем смягчить многие из проблем безопасности, которые мы могли бы найти на хостах, за которые мы несем ответственность.

Когда мы смотрим на усиление операционной системы, мы приходим к новой концепции информационной безопасности. Одной из основных целей укрепления операционной системы является уменьшение количества доступных путей, которыми может быть атакована наша операционная система. Сумма этих областей называется нашей поверхностью атаки. Чем больше наша поверхность атаки, тем больше у нас шансов на нападение[12].

Мы всегда должны проявлять большую осторожность при внесении изменений в настройки операционной системы, инструменты и программное обеспечение. Некоторые из изменений, которые мы можем внести, могут непреднамеренно повлиять на функционирование нашей операционной

системы, и на производственном компьютере это не место, чтобы узнать это на собственном опыте.

Каждая часть программного обеспечения, установленного в нашей операционной системе, добавляется к нашей поверхности атаки. Некоторые программы могут иметь гораздо больший эффект, чем другие, но все они складываются. Если мы действительно стремимся укрепить нашу операционную систему, нам нужно внимательно посмотреть на программное обеспечение, которое должно быть загружено на нее, и предпринять шаги, чтобы гарантировать, что мы работаем с минимальной необходимостью функциональной системы (диаграмма 3).

Диаграмма 3. Шесть основных способов уменьшения поверхности атаки

Удаление ненужного ПО

Например, если мы готовим веб-сервер, у нас должен быть веб-сервер, программное обеспечение, любые библиотеки или интерпретаторы кода, необходимые для поддержки веб-сервера, и любые служебные программы, связанные с администрированием и обслуживанием операционной системы, такие как программное обеспечение для резервного копирования и средства

удаленного доступа. Мы должны удалить такие приложения, как офис Microsoft или такие службы, как протокол передачи файлов (FTP). У нас действительно нет причин устанавливать что-либо еще, если система действительно будет функционировать исключительно как веб-сервер. Наши проблемы начинают возникать, когда мы видим другое программное обеспечение, установленное на машине, часто с лучшими намерениями. Например, допустим, что один из наших разработчиков входит в систему удаленно, и ему необходимо внести изменения в веб-страницу на лету, чтобы они установили необходимое программное обеспечение для веб-разработки. Затем им необходимо оценить изменения, чтобы установить свой любимый веб-браузер и соответствующие подключаемые модули мультимедиа, такие как Adobe Flash и Acrobat Reader, а также видеопроигрыватель для тестирования видеоконтента. В очень короткие сроки у нас есть не только программное обеспечение, которого там не должно быть, но оно быстро устареет, поскольку оно не исправлено, поскольку оно официально не установлено, поэтому не является частью конфигурации.

Удаление ненужных сервисов

В том же духе, что и при удалении ненужного программного обеспечения, мы также должны удалить или отключить ненужные сервисы. Многие операционные системы поставляются с широким спектром включенных служб для обмена информацией по сети, определения местоположения других устройств, синхронизации времени, обеспечения доступа к файлам и их передачи, а также выполнения других задач. Мы также можем обнаружить, что службы были установлены различными приложениями, чтобы предоставить инструменты и ресурсы, от которых зависит приложение для его функционирования.

Отключение операционных услуг может быть упражнением в экспериментах и может привести к разочарованиям. Во многих случаях такие сервисы не названы так, как указано в их действительной функции, и для

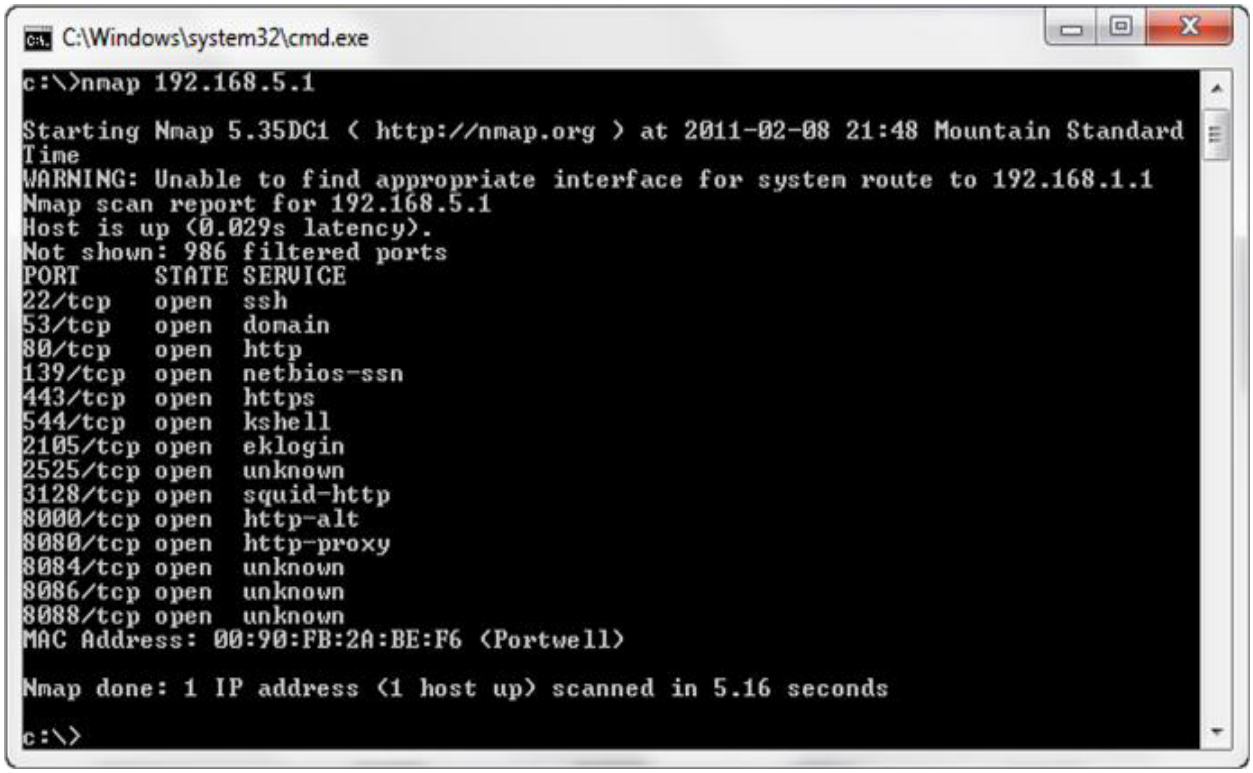
отслеживания того, что делает каждый из них, может потребоваться некоторое исследование. Одна из лучших вещей, которую нужно сделать в первую очередь, когда мы ищем такие посторонние сервисы, — это определить сетевые порты, на которых система фактически ожидает сетевые соединения. Многие операционные системы имеют встроенные утилиты, которые позволяют нам делать это, например, netstat в операционных системах Microsoft, но мы также можем использовать Nmap для таких задач.

Nmap может позволить нам обнаруживать устройства в наших сетях, но также может определять, какие сетевые порты прослушивает данная система[4].

Если мы запустим следующую команду Nmap: Nmap, IP-адрес.

Мы увидим результаты, аналогичные показанным на рисунке 2.

Рисунок 2. Проверка устройств в сети



В этом случае мы можем сразу указать несколько общих служб, работающих на цель:

• Порт 22 Удаленный доступ к системе, защищенный с помощью Secure Shell (SSH)

• Порт 53 Система доменных имен (DNS), которая переводит имеющиеся имена в IP адреса

• Порт 80 протокола передачи гипертекста (HTTP), который обслуживает веб-контент

• Порт 443 Безопасный протокол передачи гипертекста (HTTPS), который обслуживает Интернет.

Выполнять обновления

Регулярные и своевременные обновления наших операционных систем и приложений имеют решающее значение для поддержания сильной безопасности. Новые атаки публикуются на регулярной основе, и, если мы не применяем исправления безопасности, выпущенные поставщиками, которые производят наши операционные системы и приложения, мы, вероятно, станем жертвами очень большого количество известных атак.

Мы можем посмотреть на различные элементы вредоносного ПО, распространяющиеся через Интернет. Многие вредоносные программы могут распространяться, используя известные уязвимости, которые давно исправлено поставщиками программного обеспечения. Хотя стоит быть осторожным при планировании и установки обновления программного обеспечения и тщательно их протестировать, прежде чем вообще неразумно откладывать этот процесс.

Один из самых важных моментов, чтобы убедиться, что мы исправили систему непосредственно после того, как мы закончили установку. Если мы подключим недавно установленную и полностью не исправленную систему к нашей сети, мы можем увидеть, что она атакована и скомпрометированы в очень короткие сроки, даже во внутренних сетях.

В такой ситуации рекомендуется загружать патчи на съемный мультимедиа и использовать этот носитель для исправления системы, прежде чем подключать ее в сеть. Частью надежной программы управления конфигурацией является мониторинг исправлений объявления. Есть услуги, которые сделают это для вас. Вы должны также рассмотреть автоматическое исправление для систем, таких как ваш домашний компьютер.

Наконец, что не менее важно, мы должны настроить и включить соответствующую регистрацию и функции аудита для нашей системы. Настройка таких служб может незначительно отличаться в зависимости от операционной системы, а на вопрос, как использовать эту систему, мы, как правило, должны быть в состоянии вести точный и полный учет важных процессов и действий, которые происходят в наших системах. Как правило, мы хотим регистрировать важные события, такие как как осуществление административных привилегий, пользователи, входящие в систему и выходящие из нее, или когда не удается войти в систему, изменения, внесенные в операционную систему, и ряд аналогичных мероприятия. Для простой ОС Windows существует более 200 связанных с безопасностью логов, которые можно включить, поэтому важно найти правильный баланс логов и хранение. Ключевые журналы должны быть привязаны к оповещениям и программе мониторинга.

В зависимости от среды, в которой мы будем размещать систему, мы можем также захотеть включить дополнительные функции в дополнение к инструментам, встроенным в операционная систему для этих целей. Мы можем захотеть установить различные системы мониторинга инструменты, которые следят за функциональностью системы и предупреждают нас о проблемах с самой системой или аномалии, которые могут отображаться в различных системах или приложениях журналов. Мы могли бы также хотеть установить дополнительную архитектуру регистрации, чтобы контролировать деятельность нескольких машин или просто разрешить дублирование удаленной копии

журналов, которые должны храниться вне системы, чтобы гарантировать, что у нас есть неизменная запись действий, которые могли иметь место в системе.

Защита от вредоносных программ

В настоящее время большое беспокойство вызывает ошеломляющее количество и разнообразие вредоносных программ. Присутствующих в сетях, системах и устройствах хранения по всему миру. С помощью таких инструментов злоумышленники могут отключать системы, красть данные, проводить социальную инженерию атаки, шантажирование пользователей, сбор сведений и выполнение ряда других атак.

Хороший пример особенно сложного и эффективного элемента вредоносного ПО для изучения это Stuxnet. Stuxnet был впервые обнаружен в июле 2009 года, хотя и в несколько более слабой форме, чем то, чего он в конечном итоге достиг. Хотя количество системы, зараженные им, были намного ниже по сравнению с некоторыми другими вредоносными ПО. Основные вспышки вредоносных программ, которые имели место на протяжении многих лет, более конкретный акцент в том, что он был нацелен на надзорный контроль и данные системы приобретения (SCADA), которые запускают различные производственные процессы. В случае этого нападение, это было национальное государство, атакующее военный потенциал другого национального государства.

Антивирусные инструменты

Большинство антивирусных приложений обнаруживают угрозы таким же образом, как это делает IDS: путем сопоставления с сигнатурой или обнаружения аномальных действий. Средства защиты от вредоносных программ имеют тенденцию в большей степени зависеть от сигнатур, чем от обнаружения аномалий, которые обычно называются в области защиты от вредоносных программ эвристическими. Подписи вредоносного ПО обычно

обновляются поставщиком приложения не реже одного раза в день и могут обновляться чаще, чем в случае необходимости.

Средства защиты от вредоносных программ обычно обнаруживают вредоносные программы одним из двух основных способов: либо путем обнаружения наличия вредоносного ПО в реальном времени, либо с указанием трафика, либо путем сканирования файлов и процессов, уже имеющихся в системе. При обнаружении вредоносного ПО ответные меры инструмента защиты от вредоносного ПО могут включать в себя уничтожение любых связанных процессов и удаление файлов, уничтожение процессов и помещение файлов в карантин, чтобы они не могли выполняться, но не были удалены, или просто оставили все, что было обнаружено в одиночестве. Оставление файлов без изменений не является типичным ответом, но может потребоваться, поскольку средства защиты от вредоносного ПО иногда обнаруживают средства безопасности и другие файлы, которые не являются вредоносными программами, которые мы можем оставить в покое и игнорировать в будущем.

Мы можем найти средства защиты от вредоносных программ, развернутые на мобильных устройствах, отдельных системах и различных серверах, но отслеживаемые на уровне предприятия как само собой разумеющееся для крупных корпоративных сред с целью защиты этих систем. Мы также можем найти такие инструменты, установленные на прокси-серверах, чтобы отфильтровывать вредоносные программы из входящего и исходящего трафика. Это очень распространено в случае использования прокси-серверов для электронной почты, поскольку многие вредоносные программы используют электронную почту в качестве метода распространения. В случае, если вредоносным программным обеспечением обнаружен такой инструмент, мы можем увидеть, что электронное письмо полностью отклонено, или мы можем просто увидеть, как вредоносное ПО было удалено из тела сообщения или удаленное вложение было удалено.

Защита исполняемого пространства

Защита исполняемого пространства — это аппаратная и программная технология, которая может быть реализована операционными системами для предотвращения атак, использующих те же методы, которые мы обычно использовали во вредоносных программах. Короче говоря, защита исполняемого пространства предотвращает использование определенных частей памяти, используемых операционной системой и приложениями для выполнения кода. Это означает, что классические атаки, такие как переполнение буфера, которые зависят от возможности выполнять свои команды в захваченных частях памяти, могут вообще не функционировать. Многие операционные системы также используют рандомизацию размещения адресного пространства (ASLR), чтобы сместить содержимое используемой памяти так, чтобы вмешательство в нее стало еще более трудным.

Более продвинутый

Атака переполнения буфера работает путем ввода большего количества данных, чем приложение ожидает от определенного ввода, например, путем ввода 1000 символов в поле, которое ожидало только 10. В зависимости от того, как было написано приложение, мы можем обнаружить, что дополнительные 990 символы записываются где-то в память, возможно, в области памяти, используемые другими приложениями или операционной системой.

Для защиты исполняемого пространства требуются два компонента: аппаратный компонент и программный компонент. Оба основных производителя процессорных чипов, Intel и AMD, поддерживают защиту исполняемого пространства: Intel называет его битом Execute Disable (XD), а AMD - Enhanced Virus Protection.

Программная реализация защиты исполняемого пространства может быть найдена во многих распространенных операционных системах. Как предотвращение исполняемого пространства, так и ASLR можно найти во

многих операционных системах Microsoft и Apple, а также в ряде дистрибутивов Linux, и это лишь некоторые из них[2].

Программные брандмауэры и обнаружение вторжений на хост

Помимо инструментов, которые мы можем использовать в сети для обнаружения и фильтрации нежелательного трафика, таких как брандмауэры и сетевые системы обнаружения вторжений (NIDS), мы можем добавить еще один уровень безопасности на уровне хоста, реализовав здесь очень похожий набор инструментов. Несмотря на то, что мы часто можем встретить межсетевые экраны и системы обнаружения вторжений (IDS, реализованные на сетевом уровне в виде специализированных устройств, реальные функции, которые они выполняют, обычно выполняются с помощью специального программного обеспечения, установленного на устройствах. Подобное программное обеспечение может быть установлено непосредственно на хостах, находящихся в наших сетях.

Программные брандмауэры

Правильно настроенные программные брандмауэры - это очень полезный дополнительный уровень безопасности, который мы можем добавить к хостам, расположенным в наших сетях. Такие брандмауэры, как правило, содержат подмножество функций, которые мы могли бы найти на большом устройстве брандмауэра, но часто способны к очень похожей фильтрации пакетов и проверке пакетов с отслеживанием состояния.

Мы часто находим наборы правил таких приложений, выраженные в терминах конкретных приложений и портов, которым разрешено отправлять и получать трафик через различные сетевые интерфейсы, которые существуют на хосте. Такое программное обеспечение может варьироваться от относительно простых версий, которые встроены и поставляются с общими операционными системами, такими как Windows и OS X, до больших версий, предназначенных для использования в корпоративных сетях, которые включает

централизованный мониторинг и возможность значительно более сложных правил и вариантов управления.

Обнаружение вторжения на хост (HIDS)

HIDS используются для анализа действий на сетевом интерфейсе конкретного хоста или направленных на него. Они обладают многими теми же преимуществами, что и сетевые системы обнаружения вторжений (NIDS), но со значительно сокращенным объемом работы. Как и в случае программных брандмауэров, такие инструменты могут варьироваться от простого потребителя версии до гораздо более сложных коммерческих версий, которые обеспечивают централизованный мониторинг и управление.

Потенциальный недостаток HIDS с централизованным управлением состоит в том, что для того, чтобы программное обеспечение сообщало о нападении на механизм управления в режиме реального времени, информация должна передаваться по сети. Если рассматриваемый хост активно подвергается атаке через ту же сеть, о которой мы сообщаем, возможно, мы не сможем это сделать. Мы можем попытаться смягчить такие проблемы, посылая обычный маяк с устройства в механизм управления, что позволяет нам предположить проблему если, мы перестанем видеть несколько устройств неожиданно, но это может быть не полный подход.

Инструменты безопасности операционной системы

Для оценки безопасности наших хостов можно также использовать сканеры, чтобы проверить, как наши хосты взаимодействуют с остальными устройствами в сети, инструменты оценки уязвимости, чтобы помочь определить конкретные области, в которых мы можем найти приложения или службы, которые могут быть открыты для атаки, инструменты повышения привилегий для получения несанкционированного доступа. в наших системах и различных инфраструктурах эксплойтов, позволяющих нам получить доступ к широкому спектру инструментов и атак, которые могут быть использованы

теми, кто пытается подорвать нашу безопасность. Такие инструменты, не похожи на исчерпывающийся список, но мы затронем несколько основных моментов[23].

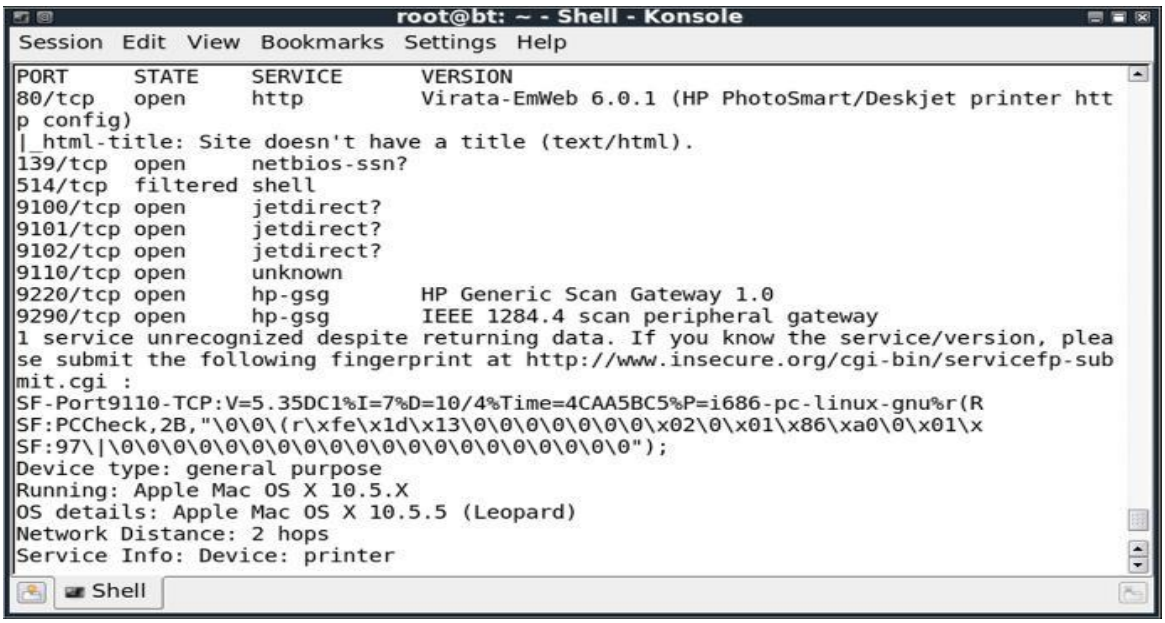
Сканеры

Мы можем использовать большое количество инструментов сканирования, чтобы помочь обнаружить различные недостатки безопасности, когда мы смотрим на хосты. Такие инструменты также можно использовать для повышения безопасности наших хостов. Мы можем искать открытые порты и версии запущенных служб, проверять баннеры, отображаемые службами, на предмет информации, проверять информацию наших систем, отображаемую по сети и выполняющее большое количество аналогичных задач.

Ранее в этой главе, когда мы обсуждали усиление защиты, мы рассмотрели очень простой пример использования Nmap для просмотра устройства в сети с целью обнаружения портов, в которых были прослушаны службы. Nmap на самом деле имеет очень большой и широкий набор функций и может дать нам значительно больше информации, если мы попросим это сделать. На рисунке 3 мы можем видеть результаты Nmap.

Сканирование направлено против сетевого принтера. В этом случае мы попросили Nmap также найти конкретные версии найденных сервисов и попытаться определить операционную систему, работающую на устройстве.

Рисунок 3. Результаты скана Nmap



Если мы посмотрим на порт 9220 в листинге, то увидим, что это сервис hp-gsg, который, хотя и немного загадочно, может дать нам некоторую подсказку, что это сервис, специфичный для принтеров HP, но если мы посмотрим на Информацию о версии в той же строке, мы можем очень четко видеть, что сервис HP Generic Scan Gateway 1.0. Основываясь на этой информации, у нас может быть гораздо больше шансов успешно атаковать устройство.

Безопасность операционной системы в реальном мире

Меры безопасности операционной системы, широко используются в компаниях по всему миру. Различные шаги, которые мы прошли, когда обсуждали усиление защиты операционных систем, обычно осуществляются любой компетентной организацией, которая создает серверы для развертывания, особенно в тех случаях, когда эти серверы будут выходить в Интернет. В зависимости от рассматриваемой организации и ее состояния безопасности, мы можем или не можем найти такие меры, чтобы иметь проводились на клиентских машинах. Несмотря на то, что такие базовые меры по обеспечению безопасности являются способом, с помощью которого мы можем сравнительно легко повысить нашу безопасность, мы делаем это за счет потенциального ущерба для простоты использования и производительности.

Использование инструментов защиты от вредоносных программ, HIDS и программных брандмауэров также довольно распространено во многих организациях любого значительного размера. Обычно на прокси-серверах будут установлены средства защиты от вредоносных программ, которые фильтруют веб-трафик и почтовый трафик по мере его поступления из Интернета. Без таких инструментов, даже если у нас очень сильная защита границ в виде межсетевых экранов и IDS, когда что-то удается сделать с помощью этих мер, это вызовет большой хаос в наших внутренних сетях.

Инструменты, которые мы обсуждали в этой главе, являются одними из основных в индустрии безопасности. Огромное количество и разнообразие таких инструментов могут быть использованы в любой конкретной среде для любого количества применений, но, если вы потратите время на изучение некоторых из наиболее часто встречающихся, таких как Nmap и Nessus, они будут полезны всем, кто входит в систему безопасности. Мы можем увидеть более крупные и дорогие коммерческие инструменты, используемые в данной среде, но они часто будут использоваться бок о бок со старыми дублерами.

Одним из основных инструментов, которые мы можем использовать в наших усилиях по обеспечению безопасности операционных систем, за которые мы несем ответственность, является усиление защиты. Основными задачами, когда мы стремимся укрепить операционную систему, являются удаление всего ненужного программного обеспечения, удаление всех несущественных служб, изменение учетных записей по умолчанию в системе, использование принципа наименьших привилегий, применение обновлений программного обеспечения соответствующим образом и вести логирование и аудит[28].

Мы также можем применять различные дополнительные уровни безопасности для наших операционных систем в форме дополнительного программного обеспечения. Мы можем установить средства защиты от вредоносных программ, чтобы обнаруживать, предотвращать и удалять

вредоносные программы при их обнаружении. Мы можем использовать технологию межсетевого экрана непосредственно на наших хостах, чтобы отфильтровывать нежелательный трафик, когда он входит или выходит из наших сетевых интерфейсов. Мы также можем установить HIDS для обнаружения атак, которые приходят на нас через сеть.

В наших усилиях по защите наших операционных систем мы можем использовать различные инструменты безопасности, чтобы найти недостатки безопасности, которые могут присутствовать. Доступен ряд инструментов сканирования, среди которых Nmap является одним из самых известных. Мы также можем использовать инструменты оценки уязвимостей, чтобы найти конкретные недостатки безопасности в наших сервисах или программном обеспечении с поддержкой сети, например Nessus. Кроме того, мы можем использовать среды эксплойтов для атаки на системы, пытаясь получить к ним доступ или получить повышенные уровни привилегий, при этом Metasploit является одним из наиболее известных инструментов.

ГЛАВА II. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Принципы, методы, подходы и средства обеспечения безопасности

Деятельность организации в области информационной безопасности будет успешной, только если она работает в сочетании с политикой информационной безопасности организации. Программа информационной безопасности начинается с политики, стандартов и практик, которые являются основой архитектуры информационной безопасности. Создание и поддержание этих элементов требует скоординированного планирования. Роль планирования в современной организации трудно переоценить. Все организации, кроме самых маленьких, занимаются определенным планированием: стратегическим планированием для управления распределением ресурсов и планированием на случай непредвиденных обстоятельств, чтобы подготовиться к неопределенности бизнес-среды.

Планирование и управление информационной безопасностью

Стратегическое планирование определяет долгосрочное направление деятельности всей организации и каждой ее составной части. Стратегическое планирование должно направлять организационные усилия и направлять ресурсы на достижение конкретных, четко определенных целей. После того, как организация разрабатывает общую стратегию, она генерирует общий стратегический план, распространяя эту общую стратегию на стратегические планы для основных подразделений. Каждый уровень каждого подразделения затем переводит эти цели плана в более конкретные цели для уровня ниже. Чтобы реализовать эту широкую стратегию и воплотить общую стратегию в действие, исполнительная группа (иногда называемая C-уровнем организации, как в CEO, COO, CFO, CIO и т. Д.) должна сначала определить индивидуальные обязанности. Преобразование целей с одного стратегического уровня на следующий, более низкий уровень, возможно, больше искусство, чем наука.

Он опирается на способность руководителя знать и понимать стратегические цели всей организации, знать и оценивать стратегические и тактические способности каждого подразделения в организации, а также вести переговоры со сверстниками, начальством и подчиненными. Такое сочетание навыков помогает достичь правильного баланса между целями и возможностями.

Уровни планирования

После того, как общий стратегический план организации переведен в стратегические планы для каждого основного подразделения или операции, следующим шагом является преобразование этих планов в тактические цели, направленные на достижение конкретных, измеримых, достижимых и ограниченных по времени достижений.

Процесс стратегического планирования стремится трансформировать широкие, общие, широкие утверждения в более конкретные и прикладные цели. Стратегические планы используются для создания тактических планов, которые в свою очередь используются для разработки оперативных планов.

Тактическое планирование сосредоточено на краткосрочных мероприятиях, которые будут завершены в течение одного или двух лет. Процесс тактического планирования разбивает каждую стратегическую цель на ряд дополнительных задач. Каждая цель в тактическом плане должна быть конкретной и должна иметь дату доставки в течение года после начала плана. Составление бюджета, распределение ресурсов и персонал являются важными компонентами тактического плана. Хотя эти компоненты могут обсуждаться в общих чертах на уровне стратегического планирования, фактические ресурсы должны быть в наличии, прежде чем тактический план может быть преобразован в оперативный план. Тактические планы часто включают планы проекта и документы по планированию приобретения ресурсов (например, спецификации продукта), бюджеты проектов, обзоры проектов, а также ежемесячные и годовые отчеты.

Поскольку тактические планы часто создаются для конкретных проектов, некоторые организации называют этот процесс планированием проекта или промежуточным планированием. Главный сотрудник по информационной безопасности (CISO) и менеджеры по безопасности используют тактический план для организации, определения приоритетов и получения ресурсов, необходимых для крупных проектов, а также для поддержки общего стратегического плана.

Менеджеры и сотрудники используют оперативные планы, основанные на тактических планах, для организации текущего повседневного выполнения задач. Операционный план включает в себя необходимые задачи для всех соответствующих отделов, а также требования к коммуникации и отчетности, которые могут включать еженедельные совещания, отчеты о ходе работы и

другие связанные задачи. Эти планы должны отражать организационную структуру, при этом каждое подразделение, отдел или проектная группа осуществляет свое собственное оперативное планирование и отчетность. Частое общение и обратная связь от команд к менеджерам проектов и / или руководителям команд, а затем вплоть до различных уровней управления, сделает процесс планирования в целом более управляемым и успешным[1].

Планирование и CISO

Первоочередной задачей CISO и группы управления информационной безопасностью является создание стратегического плана для достижения целей информационной безопасности организации. Хотя каждая организация может иметь свой собственный формат для разработки и распространения стратегического плана, основные элементы планирования имеют общие характеристики для всех типов предприятий. План представляет собой развивающееся заявление о том, как CISO и различные элементы организации будут реализовывать цели информационной безопасности, которые выражены в политике информационной безопасности предприятия (EISP).

Управление информационной безопасностью

Управление — это совокупность обязанностей и практики, которые выполняются советом и исполнительным руководством с целью обеспечения стратегического руководства, обеспечения достижения целей, обеспечения надлежащего управления рисками и проверки того, что ресурсы предприятия используются ответственно. Управление описывает весь процесс управления или контроля процессов, используемых группой для достижения какой-либо цели.

Точно так же, как у правительств, корпораций и других организаций есть руководящие документы - корпоративные уставы или соглашения о партнерстве, а также назначенные или избранные руководители или должностные лица, а также процедуры планирования и работы. Эти элементы в

сочетании обеспечивают корпоративное управление. Каждое действующее подразделение в организации также имеет контроль над обычаями, процессами, комитетами и практикой. Руководство группы информационной безопасности контролирует и управляет всеми организационными структурами и процессами, обеспечивающими защиту информации. Управление информационной безопасностью, таким образом, представляет собой применение принципов корпоративного управления, то есть ответственность исполнительного руководства за обеспечение стратегического направления, обеспечение достижения целей, контроль над надлежащим управлением рисками и проверку ответственного использования ресурсов - для информационной безопасности.

Управление информационной безопасностью является обязанностью стратегического планирования, значение которой возросло за последние годы. К сожалению, информационная безопасность слишком часто рассматривается как техническая проблема, когда на самом деле это проблема управления. Чтобы защитить информационные активы, руководство организации должно интегрировать методы информационной безопасности в структуру организации, расширяя политики корпоративного управления и средства управления, чтобы охватить цели процесса информационной безопасности.

Цели информационной безопасности должны решаться на самом высоком уровне управленческой команды организации, чтобы быть эффективной и устойчивой. Когда программы безопасности разрабатываются и управляются в качестве технической специальности в ИТ-отделе, они с меньшей вероятностью будут эффективными. Более широкий взгляд на информационную безопасность охватывает все информационные активы организации, включая знания, которыми управляют эти ИТ-активы. Ценность информационных активов организации должна быть защищена независимо от того, как данные в ней обрабатываются, хранятся или передаются, а также с полным пониманием рисков и преимуществ информационных активов. Согласно Институту

управления информационными технологиями (ITGI), управление информационной безопасностью включает в себя все обязанности и методы, используемые советом директоров и исполнительным руководством для обеспечения стратегического руководства, установления целей, измерения прогресса в достижении этих целей, проверки того, что управление рисками соответствующие практики, и проверка того, что активы организации используются должным образом.

Структура управления

Для эффективной реализации управления безопасностью целевая группа по корпоративному управлению (CGTF) рекомендует организациям следовать установленной структуре, такой как структура IDEAL от Института разработки программного обеспечения Университета Карнеги-Меллона. Эта структура, которая описана в документе Управление информационной безопасностью: призыв к действию, определяет обязанности

- совета директоров или заместителей,
- старшего исполнительного директора организации (т.е. генерального директора),
- исполнительного органа члены команды,
- старшие менеджеры
- все сотрудники и пользователи.

Политика, стандарты и практика информационной безопасности

Управление всеми заинтересованными сообществами, включая общий персонал, информационные технологии и информационную безопасность, должно сделать политики основой для всего планирования, проектирования и развертывания информационной безопасности. Политики определяют, как следует решать проблемы и использовать технологии. Политики не определяют правильное функционирование оборудования или программного обеспечения -

эта информация должна быть размещена в стандартах, процедурах и методах руководств пользователя и системной документации. Кроме того, *политика никогда не должна противоречить закону*, поскольку это может создать значительную ответственность для организации.

Программы обеспечения качества начинаются и заканчиваются политикой. Информационная безопасность — это, прежде всего, проблема управления, а не техническая проблема, а политика - это инструмент управления, который обязывает персонал функционировать таким образом, который обеспечивает безопасность информационных активов. Политики безопасности являются наименее дорогостоящим элементом управления, но наиболее сложным для реализации *правильной*.

Они имеют самую низкую стоимость в том смысле, что их создание и распространение требуют только времени и усилий команды управления. Даже если управленческая команда нанимает внешнего консультанта для разработки политики, затраты минимальны по сравнению с техническими средствами контроля[7].

Политика представляет собой план или курс действий, который передает инструкции от высшего руководства организации к тем, кто принимает решения, принимает меры и выполняет другие обязанности. Политики — это организационные законы в том смысле, что они диктуют приемлемое и неприемлемое поведение внутри организации. Как и законы, политики определяют, что правильно, что неправильно, какие наказания за нарушение политики и каков процесс апелляции.

Стандарты, с другой стороны, являются более подробным изложением того, что должно быть сделано для соблюдения политики. Они имеют те же требования к соответствию, что и политики. Стандарты могут быть неформальными или частью организационной культуры, как в стандартах де-факто. Либо стандарты могут быть опубликованы, тщательно изучены и

ратифицированы группой, как в официальных или стандартах де-юре. Наконец, практики, процедуры и руководства эффективно объясняют, как соблюдать политику.

Политики создаются для поддержки миссии, видения и стратегического планирования организации.

Миссия организации является письменным заявлением цели организации.

Видение организации является письменное заявление об организации целей, где будет организация через пять лет? В десять? Стратегическое планирование — это процесс продвижения организации к ее видению.

Смысл термина **политика безопасности** зависит от контекста, в котором он используется. Правительственные органы рассматривают политику безопасности с точки зрения национальной безопасности и национальной политики в отношении иностранных государств. Политика безопасности также может сообщать метод агентства кредитных карт для обработки номеров кредитных карт. В общем, политика безопасности - это набор правил, которые защищают активы организации.

Политика информационной безопасности устанавливает правила защиты информационных активов организации.

Руководство должно определить три типа политики безопасности:

1. Политики информационной безопасности предприятия

2. Специфичные для проблемы политика безопасности,

3.Специфичные для системы.

Чтобы политика была эффективной и, следовательно, имела юридическую силу, она должна отвечать следующим критериям:

Распространение - Организация должна иметь возможность продемонстрировать, что политика была легко доступна для проверки

работник. Общие методы распространения включают в себя печатные копии и электронное распространение.

Проверка (чтение) - Организация должна иметь возможность продемонстрировать, что она распространяла документ в доступной форме, включая версии для неграмотных, не говорящих по-английски сотрудников и работников с нарушениями чтения. Общие методы включают запись политики на английском и других языках.

Понимание (понимание) - Организация должна быть в состоянии продемонстрировать, что сотрудник понимает требования и содержание политики. Общие методы включают в себя тесты и другие оценки.

Соблюдение (соглашение) - Организация должна быть в состоянии продемонстрировать, что работник соглашается соблюдать политику, посредством действия или подтверждения. Обычные методы включают в себя баннеры входа в систему, которые требуют определенного действия (щелчок мыши или нажатие клавиши) для подтверждения соглашения, или подписанный документ, четко указывающий, что сотрудник прочитал, понял и согласился соблюдать политику[16].

Равномерное правоприменение - организация должна быть в состоянии продемонстрировать, что политика применялась единообразно, независимо от статуса или назначения сотрудника.

Политика информационной безопасности предприятия (EISP) также известна в качестве общей политики безопасности, политики безопасности организации, ИТ политики безопасности или политики информационной безопасности. EISP основана и напрямую поддерживает миссию, видение и направление организации и определяет стратегическое направление, масштаб и тон для всех мер безопасности. EISP — это документ исполнительного уровня, обычно составляемый главным исполнительным директором организации или в сотрудничестве с ним. Эта политика обычно занимает от двух до десяти

страниц и формирует философию безопасности в ИТ-среде. EISP, как правило, необходимо модифицировать только в случае изменения стратегического направления организации.

EISP направляет разработку, внедрение и управление программой безопасности. В нем изложены требования, которым должен соответствовать проект или инфраструктура информационной безопасности. Он определяет цель, область применения, ограничения и применимость программы безопасности. Он также назначает обязанности для различных областей безопасности, включая системное администрирование, поддержку политик информационной безопасности, а также практики и обязанности пользователей. Наконец, это касается соблюдения законодательства. Согласно Национальному институту стандартов и технологий (NIST), EISP, как правило, рассматривает соответствие в следующих двух областях:

1. Общее соответствие, чтобы обеспечить выполнение требований по созданию программы и обязанностей, возложенных на нее различными организационными компонентами

2. Использование определенных штрафов и дисциплинарных мер.

Когда EISP был разработан, CISO начинает формировать команду безопасности и инициировать необходимые изменения в программе информационной безопасности.

Элементы EISP, хотя специфика EISP варьируется от организации к организации, большинство документов EISP должны включать следующие элементы[27]:

- Обзор корпоративной философии безопасности
- Информация о структуре организации информационной безопасности и физических лиц, которые выполняют роль информационной безопасности

- Полностью сформулированные обязанности по обеспечению безопасности, которые разделяют все члены организации (сотрудники, подрядчики, консультанты, партнеры и посетители)
- Полностью сформулированные обязанности по обеспечению безопасности, которые являются уникальными для каждой роли в организации

Специфичная для проблемы политика безопасности (ISSP)

Поскольку организация использует различные технологии и процессы для поддержки рутинных операций, она должна проинструктировать сотрудников о правильном использовании этих технологий и процессов. В целом политика безопасности для конкретной проблемы, или ISSP, затрагивает конкретные области технологии, перечисленные ниже, требует частых обновлений и содержит заявление о позиции организации по конкретному вопросу. ISSP может охватывать следующие темы, среди прочего:

- E-mail
- Использование Интернета
- Конкретные минимальные конфигурации компьютеров для защиты от червей и вирусов
- Запреты на взлом или тестирование контроля безопасности организации
- Домашнее использование принадлежащего компании компьютерного оборудования
- Использование личного оборудования в сетях компании
- Использование телекоммуникационных технологий (факс и телефон)
- Использование фотокопировального оборудования

Существует несколько подходов к созданию и управлению ISSP в организации.

Три наиболее распространенных из них:

1. Независимые документы ISSP, каждый из которых предназначен для конкретной проблемы

2. Единый всеобъемлющий документ ISSP, охватывающий все вопросы

3. Модульный документ ISSP, который объединяет создание политики и администрирование, поддерживая при этом требования каждой конкретной проблемы.

Независимый Документ ISSP обычно имеет эффект рассеяния. Каждый отдел, ответственный за конкретное применение технологии, создает политику, регулирующую ее использование, управление и контроль. Этот подход может не охватить все необходимые проблемы и может привести к плохому распределению политики, управлению и обеспечению соблюдения. Единый комплексный ISSP централизованно управляется и контролируется. С введением формальных процедур управления ISSP, комплексный политический подход устанавливает руководящие принципы для общего охвата необходимых вопросов и четко определяет процессы для распространения, обеспечения соблюдения и анализа этих руководящих принципов. Обычно эти политики разрабатываются лицами, ответственными за управление ресурсами информационных технологий. К сожалению, эти политики имеют тенденцию чрезмерно обобщать проблемы и пропускать уязвимости. Оптимальным балансом между независимым и всеобъемлющим ISSP является модульный ISSP. Он также централизованно управляется и контролируется, но с учетом индивидуальных технологических проблем.

Модульный подход обеспечивает баланс между ориентацией на проблемы и управлением политикой. Политики, созданные с помощью этого подхода, содержат отдельные модули, каждый из которых создается и обновляется людьми, ответственными за решаемые проблемы. Эти люди подчиняются группе централизованного управления политикой, которая включает конкретные вопросы в общую комплексную политику. Организация

должна добавить к этой структуре конкретные детали, которые определяют процедуры безопасности, не охватываемые этими общими руководящими принципами.

Заявление о политике Политика должна начинаться с четкого изложения цели. Рассмотрим политику, которая охватывает проблему справедливого и ответственного использования Интернета. Во вводном разделе этой политики должны быть изложены следующие темы: Какова область действия этой политики? Кто несет за реализацию политики? Какие технологии и проблемы она решает?

Санкционированный доступ и использование оборудования. В этом разделе рассматривается, *кто* может использовать технологию, регулируемую политикой, и для *чего* она может использоваться. Помните, что информационные системы организации являются исключительной собственностью организации, и пользователи не имеют особых прав на использование. Каждая технология и процесс предназначены для бизнес-операций. Использование для любых других целей представляет собой неправильное использование оборудования.

Запрещенное использование оборудования. Если конкретное использование явно не запрещено, организация не может наказать своих сотрудников за неправильное использование. Следующее может быть запрещено: личное использование, деструктивное использование или неправомерное использование, преступное использование, оскорбительные или преследующие материалы, а также нарушение авторских прав, лицензий или другой интеллектуальной собственности.

2.2. Организационно-техническое обеспечение компьютерной безопасности

Физическая безопасность в значительной степени связана с защитой трех основных категорий активов: людей, оборудования и данных. Нашей главной задачей, конечно же, является защита людей. Людей значительно труднее

заменить, чем оборудование или данные, особенно если они имеют опыт работы в своей конкретной области и знакомы с процессами и задачами, которые они выполняют.

Далее в порядке приоритета защиты находятся наши данные. Если мы достаточно спланировали и подготовились заранее, мы сможем легко защитить наши данные от любого бедствия, которое не имеет глобального масштаба. Если мы не подготовимся к такой проблеме, можем очень легко потерять наши данные навсегда. Как правило, мы не можем и не должны разрабатывать планы безопасности, которые защищают одну из этих категорий в отрыве от других.

Это может показаться очень важным набором объектов, которым мы могли бы хотеть назначить более высокий уровень приоритета при планировании наших мер физической безопасности. Однако, как правило, это не так, за исключением нескольких ситуаций, большинство из которых на самом деле связаны с обеспечением безопасности людей. В мире технологий большая часть используемого нами оборудования является относительно общей и легко заменяется. Даже если мы используем более специализированное оборудование, мы часто можем заменить его в считанные дни или недели. Во многих крупных организациях защита людей, данных и оборудования охватывается набором политик и процедур, которые в совокупности называются планированием непрерывности бизнеса (BCP) и планированием аварийного восстановления (DRP), часто называемым одним объектом, называемым BCP / DRP. BCP конкретно относится к планам, которые мы разработали, чтобы гарантировать, что важнейшие бизнес-функции могут продолжать работу в условиях чрезвычайного положения. DRP охватывает планы, которые мы разработали для подготовки к потенциальной катастрофе, и что именно мы будем делать во время и после конкретной катастрофы, чтобы заменить инфраструктуру.

Основные категории физических угроз.

Угрозы, с которыми мы сталкиваемся, когда имеем дело с физической безопасностью, обычно делятся на несколько основных категорий, перечисленных ниже:

• Экстремальные температуры

• Газы

• Жидкости

• Живые организмы

• Снаряды

• Движение

• Энергетические аномалии

• Люди

• Токсины

• Дым и огонь

Первые семь из этих категорий - экстремальные температуры, газы, жидкости, живые организмы, снаряды, движения и энергетические аномалии - были определены Донном Паркером в его книге Борьба с компьютерными преступлениями.

Средства физической безопасности — это устройства, системы, люди и другие методы, которые мы применяем для обеспечения нашей безопасности в физическом смысле. Существует три основных типа физического контроля: сдерживающий, детективный и превентивный. Каждый из них имеет разную направленность, но ни один не является полностью отличным и отдельным от других, как мы вскоре обсудим. Кроме того, эти элементы управления работают лучше всего при использовании на концерте. Ни одного из них недостаточно для обеспечения нашей физической безопасности в большинстве ситуаций.

Физические проблемы с данными

В зависимости от типа физического носителя, на котором хранятся наши данные, любое количество неблагоприятных физических условий может быть проблематичным или вредным для их целостности.

Такие среды часто чувствительны к температуре, влажности, магнитным полям, электричеству, ударам и многим другим, причем каждый тип среды имеет свои сильные и слабые стороны.

Магнитные носители, независимо от того, ссылаемся ли мы на жесткие диски, ленты, дискеты или иные, обычно включают в себя некоторое разнообразие движущихся и магнитных чувствительных материалов, на которые записываются данные. Сочетание магнитной чувствительности и движущихся частей часто делает хрупкими таких носителей так или иначе. В большинстве случаев сильные магнитные поля могут нанести ущерб целостности данных, хранящихся на магнитных носителях, причем носители вне металлического корпуса, такие как магнитные ленты, еще более чувствительны к таким нарушениям. Кроме того, тряска таких носителей, когда они находятся в движении, обычно во время их чтения или записи, может иметь множество нежелательных эффектов, что часто делает носителя непригодным для использования.

Флэш-носители, относящиеся к общей категории носителей, в которых хранятся данные на энергонезависимых микросхемах памяти, на самом деле довольно выносливы. Если нам удастся избежать ударов, которые могут непосредственно сломать микросхемы, на которых хранятся данные, и мы не подвергнем их электрическим ударам, они, как правило, будут противостоять условиям, которые не будут допускать многие другие типы носителей. Они не очень чувствительны к температурным диапазонам ниже того, что могло бы фактически разрушить корпус, и часто выдерживают кратковременное погружение в жидкость, если впоследствии их правильно высушить. Некоторые флэш-накопители предназначены специально для того, чтобы выдерживать экстремальные условия, которые обычно разрушают такие носители, для тех, кто может считать такие условия потенциальной проблемой.

Оптические носители, такие как компакт-диски и DVD-диски, являются довольно хрупкими, что могут засвидетельствовать те, у кого есть маленькие

дети или домашние животные. Даже небольшие царапины на поверхности носителя могут сделать его непригодным для использования. Он также очень чувствителен к температуре, так как изготовлен в основном из пластика и тонкой металлической фольги. Вне защищенной среды такой как специальное хранилище носителей, любая из множества угроз может уничтожить данные на таких носителях.

Дополнительным фактором, который может потенциально вызывать беспокойство при работе с носителями данных в течение длительного периода времени, является технический износ. Тип носителя, программное обеспечение, интерфейсы и другие факторы могут повлиять на нашу способность читать хранимые данные. Например, Sony прекратила производство дискет в марте 2011 года, так как на нее было возложено 70% оставшегося производства таких носителей. Хотя дискеты только сейчас полностью исчезают из-за использования, очень мало новых компьютеров, которые оснащены дисководами для их чтения. Через несколько коротких лет найти аппаратное обеспечение для чтения этих дисков станет очень сложно.

Доступность

Одной из наших главных задач при обсуждении защиты данных является обеспечение доступности данных для нас, когда нам необходим доступ к ним. Доступность наших данных часто зависит как от нашего оборудование, так и от наших средств, которые находятся в рабочем состоянии. Любые физические проблемы, которые мы обсуждали ранее, могут сделать наши данные недоступными в том смысле, что они могут считываться с носителя, на котором они хранятся. Хотя мы специально обсуждаем здесь доступ к данным и обсуждали некоторые потенциальные проблемы с оборудованием при доступе к определенным типам носителей ранее, есть также довольно существенный компонент оборудования и инфраструктуры, который следует учитывать при обсуждении доступности. Мы можем не только столкнуться с проблемами при чтении данных с носителя, но и с доступом к месту хранения данных. Если в

какой-то момент между нашим местоположением и удаленным хранилищем данных у нас возникнет сбой, связанный с сетью, питанием, компьютерными системами или другими компонентами, мы не сможем получить удаленный доступ к нашим данным. Сегодня многие компании работают по всему миру, и вполне возможно, что потеря возможности удаленного доступа к данным, даже временно, будет довольно серьезной проблемой.

ГЛАВА III. ИНФОРМАЦИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ И ОРГАНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ

3.1. Автоматизированные информационные системы (АИС) в экономике

Было выявлено что, фактически используемые предприятиями учетные информационные системы сильно отличаются от компании к компании и от банка к банку. Более крупные компании или банки обычно используют более сложные системы, чем небольшие компании или банки. Типы экономических событий, влияющих на компании, также вызывают различия в системах. Эту точку зрения поддерживает и Kieso, который определил АИС следующим образом: собирает и обрабатывает данные о транзакциях, а затем распространяет финансовую информацию среди заинтересованных сторон. Информационные системы бухгалтерского учета широко варьируются от одного предприятия к другому. Эти системы определяют различные факторы: характер бизнеса и операций, в которых он участвует, размер фирма, объем данных, которые необходимо обработать и информационные требования, которые требуются руководству и другим лицам.

В то же время Ангел Холл рассматривает АИС как подсистемы, обрабатывающие финансовые транзакции и нефинансовые переходы, которые напрямую влияют на обработку финансовых транзакций.

Все вышеперечисленные пункты показывают, что АИС - это системы, основные системы, различные системы или даже подсистемы, с которыми все они встречались, и согласование системы слов, которая помогает любой организации собирать различные данные, обрабатывать их и распространять среди лиц, принимающих решения. АИС нуждается в технологии, чтобы быть точной, надежной и в срок. Правой рукой для выполнения миссий АИС в любой организации является информационная безопасность. Понимать термин информационная безопасность и преимущества для банков и АИС в том, что касается преактивной работы с рисками безопасности, такими как: принятие политики информационной безопасности в отношении обработки конфиденциальных данных, наличие процедур для сообщений об инцидентах безопасности, информирование сотрудников о своих обязанностях.

Информационная безопасность относится ко всем процедурам, которые используются для защиты информации от преднамеренного или случайного неправильного использования или распространения. Технически это относится к поддержанию целостности информации. Целостность означает, что информация всегда остается верной и не может быть доступна неавторизованным агентам.

Для бизнеса существует целая темная область, известная как промышленный шпионаж, в которой используются различные средства для раскрытия коммерческой тайны и ведения бизнеса. Очевидно, что существует абсолютная необходимость в сохранении конфиденциальности всей информации компании. Менее очевидное нарушение информационной безопасности происходит из-за промышленного шпионажа, где информация либо изменяется, либо удаляется, чтобы саботировать функционирование организации. Когда на карту поставлена проблема информационной

безопасности, необходимо принять во внимание три фундаментальных понятия:

1. Конфиденциальность

2. Доступность

3. Целостность.

Эти цели помогут прояснить, что в целом должно быть защищено, и причины для этого.

Атаки на конфиденциальность информации связаны с хищением или несанкционированным доступом к данным. Это может происходить разными способами, такими как перехват данных во время их передачи или просто кража устройств, на которых хранятся данные. Целью нарушения конфиденциальности является получение конфиденциальной информации, использование учетных данных, удаление секретной, финансовой, медицинской или другой информации.

Доступность позволяет законному пользователю получить доступ к конфиденциальной информации после ее надлежащей аутентификации. Когда доступность скомпрометирована, доступ может даже быть отказан законным пользователям из-за злонамеренных действий, таких как атаки типа отказ в обслуживании (DoS).

Целостность подразумевает несанкционированное изменение информации. Это также может означать изменения в информации, когда она находится в пути или хранится в какой-либо форме поддержки. Чтобы защитить целостность информации, должны быть внедрены эффективные методы проверки. Этими методами могут быть проверки целостности или цифровые подписи.

Угрозы, с которыми сталкиваются банки и АИС, могут классифицироваться как внутренние угрозы и внешние угрозы. Внутренние

угрозы исходят от кого-то, работающего внутри банков, тогда как внешние угрозы исходят от внешнего лица[3].

1. **Внутренние угрозы:**

Ложные счета. Банковские власти могут открывать фальшивые счета на имена фиктивных клиентов и предоставлять привилегии этой учетной записи. Они могут предоставлять такие счета в виде займов и кредитов. Позже они могут конвертировать эти деньги в личное пользование.

Мошеннические кредиты. Одним из способов получения наличных в банке является получение кредита. Мошеннический заем — это один из способов, где заемщик работает на банк или помощника и взяв кредит он сообщает о банкротстве или просто исчезает, что в конечном итоге приводит к потере денег. Заемщик может даже быть несуществующим юридическим лицом, и кредит - всего лишь уловка, чтобы скрыть кражу большой суммы наличных денег из банка.

Проводное мошенничество сети. Передачи данных, такие как универсальный SWIFT и Межбанковский перевод средств всегда является целью, потому что, если перевод сделан, это трудно или не подлежит обращению. Инсайдеры могут создавать риски, пытаясь использовать мошеннические или фальшивые документы, которые требуют, чтобы денежные средства вкладчика банка были переведены в другой банк, всегда находящийся на счете в каком-либо отдаленном зарубежном государстве.

Поддельные или мошеннические документы. Фальшивые документы всегда используются, чтобы скрыть другие грабежи. Банки, как правило, рассчитывают свои наличные деньги точно, поэтому каждый счет должен учитываться. Таким образом, документ, утверждающий, что сумма наличных была заимствована в качестве займа, выданного кем-то (вкладчиком) или передана или инвестирована, может, таким образом, быть достойным банкира,

который желает скрыть мелкие детали и предположить, что наличные были потерты и теперь потерян.

Кража личных данных. Известно, что нечестный сотрудник банка раскрывает личную информацию вкладчика для использование эту информацию при мошенничестве с кражей личных данных. Затем преступники используют эту информацию для получения удостоверений личности и кредитных карт, используя имя и личную информацию жертвы.

Мошенничество по требованию-это мошенничество обычно совершается одним или несколькими нечестными сотрудниками банка. Они удаляют из бумаги несколько документов по требованию или записей и пишут их как обычный нужный им. Поскольку они являются сотрудниками, они знают, как кодировать и составлять проект требования. Эти черновики по требованию будут выпущены к оплате в отдаленном городе где счета не дебетованы, и будут обналичены в разделе к оплате. Для платящего филиала это просто еще один проект спроса. Этот вид мошенничества будет обнаружен только в том случае, если в главном офисе будут выполнены примерочные работы, что обычно занимает 6 месяцев. К тому времени деньги уже не подлежат возврату.

2. **Внешние угрозы:**

Это угрозы со стороны и могут быть совершены кражами или хакерами. Кто-то, использующий интернет-банкинг для транзакций, должен быть осторожен с хакерами. Защитный номер и пароль являются важной информацией для вашей онлайн-транзакции, некоторые из перечисленных ниже угроз.

Мошенничество с кредитными картами. Как правило, мошенник использует кредитную карту другого лица для оплаты покупки. Некоторые из мошенничества с кредитными картами — это мошенничество с украденными

картами, мошенничество с захватом учетной записи, мошенничество с заказами по кредитной карте и скимминг.

Мошенничество с украденной кредитной картой. Когда клиент теряет карту, он может совершать несанкционированные платежи по карте, пока карта не будет аннулирована.

Мошенничество с захватом аккаунта. Мошенники звонят и подражают фактическим держателям карт, используя их украденную личную информацию. У них есть адрес и другая информация владельца карты, измененная на адрес, который они контролируют. Дополнительные карты и, возможно, почтовые программы с PIN-кодом запрашиваются и выдаются на новый адрес и используются мошенниками для совершения покупок или получения денежных авансов.

Мошенничество с заказом по кредитной карте. Используя украденный номер кредитной карты или компьютерный номер, вор закажет украденные товары.

Скимминг. Скимминг — это кража кредитной карты и информации нечестным сотрудником; это обычно делается в барах или ресторанах. Эти люди либо копируют номера вручную, либо используют считыватель магнитных полос, чтобы получить код безопасности карты.

Фишинг или мошенническая почта. Фишинг — это метод мошенничества, используемый для того, чтобы заставить людей сообщать свои номера безопасности и пароль мошенникам. Хакер отправляет мошенническое письмо, специально предназначенное для раскрытия информации о безопасности предполагаемому лицу. Это письмо разработано таким образом, что выглядит так, как будто оно пришло из ответственного источника, например; ваш банк. Это письмо может также предоставить вам гиперссылку с домашним адресом вашего банка, который снова является сайтом мошенничества. Вы можете найти этот поддельный сайт точно таким же, как и

оригинальный, на котором вы легко можете сообщить свои данные о безопасности хакеру или мошеннику. Как можно избежать фишинга, указано ниже:

Во-первых, ни один банк никогда не отправит письмо с вопросом о вашем номере безопасности и пароле. Если вы получаете письмо от своего банка, независимо от того, насколько срочно оно, никогда не помещайте в него информацию о безопасности. Всегда звоните по номеру телефона банка, чтобы проверить, хотят ли они эту информацию.

Во-вторых, если вы подозреваете, что это мошенничество, отправьте его по почте в банк, сообщив об этом мошенничестве.

Проверьте безопасность банковского сайта. Никогда не нажимайте на гиперссылку или не переходите по ссылке, чтобы перейти на домашний адрес своего банка в Интернете. Всегда вводите полный адрес вашего банка в браузере. Проверьте начинается ли сайт банка с https и есть ли значок замка в нижней части вашего браузера. Если дважды щелкнуть значок замка, появится информация о замке, что поможет вам подтвердить подлинность этого сайта. Если блокировка недействительна или была выпущена для веб-сайта, который вы не распознаете, не вводите информацию о безопасности.

Вход и выход. Не предоставляйте свои идентификатор и пароль для всех, чтобы избежать мошенничества. Не оставляйте свой компьютер или ноутбук без присмотра, пока вы все еще подключены к интернет-банкингу. Всегда выходить из системы, когда сессия закончена. Не сохраняйте идентификатор безопасности и пароль на своем компьютере и всегда храните его в надежном месте. Кроме того, не меняйте свои данные безопасности, когда вы используете компьютер в публичном месте.

3.2. Современные приложения безопасности в банках и учетных информационных системах (АИС)

Одна из самых больших проблем для многих компьютерных систем сегодня — это программное обеспечение, работающее на нем. Независимо от

того, является ли это программное обеспечение операционной системой, службой, предоставляемой операционной системой, приложением или базой данных, необходимо предпринять усилия для предотвращения уязвимостей и компрометации системы. В следующих разделах описаны минимальные шаги для защиты основных программных компонентов систем АИС и банков[21].

Укрепление и исправление операционной системы. Операционные системы загружаются группами системной инженерии среднего уровня или групп поддержки настольных систем и следуют стандартной процедуре, которая включает в себя развитие передового опыта и интеграцию соответствующих исправлений, определенных Mid-Tier, сотрудником службы информационной безопасности и SOS.

Существующие системы должны получать обновления на периодической основе, как это определено группами MTI, Database и LAN / Desktop. Любое обновление определено как критическое должны быть применены к системам в течение недели после выпуска от поставщика. Группы MTI, Database и LAN / Desktop отвечают за то, чтобы тестирование исправлений выполнялось до установки. В настольных системах установка этих обновлений должна быть по возможности автоматизирована.

Стандарты проверки подлинности. Вся проверка подлинности пользователя для ограниченного доступа выполняется с помощью фильтров Web Access, двухфакторной проверки подлинности (в соответствии с указаниями руководства АИС) или путем подтверждения комбинаций идентификатора пользователя и пароля в централизованно управляемом хранилище учетных записей пользователей ITS. Авторизация выполняется в сочетании с определениями групп в хранилище ITS LDAP, где это возможно. Если авторизация LDAP невозможна, методы авторизации могут осуществляться с помощью безопасности на уровне ОС, базы данных или приложения.

Защита приложений. Для приложений, разработанных вне организации, сотрудники Penn State, отвечающие за поддержку приложений, должны постоянно информировать персонал службы поддержки АИС об обновлениях, связанных с безопасностью. Внедрение таких обновлений должно быть согласовано с группой MTI.

Сканирование уязвимостей приложений и веб-приложений. Все приложения, размещенные в АИС, будут первоначально проверяться на наличие уязвимостей и проблем веб-приложений (если применимо) на наличие уязвимостей до первоначального развертывания. Продолжение периодического сканирования должно выполняться после этого в системах в производственных средах. Все серверы должны использовать наборы шифрования и шифров, утвержденные сотрудником АИС по информационной безопасности и старшим директором.

Брандмауэры. Брандмауэр — это первая линия защиты от хакеров. Это компьютерная программа, установленная на компьютере, который подключает сеть к Интернету. Брандмауэр анализирует пакеты, которые проходят и выходят из сети. Он запрограммирован на соблюдение определенных правил, которые позволяют ему решать, разрешать или нет пропуск пакета. Существует программное обеспечение брандмауэра, которое может быть установлено на автономном ПК.

Права доступа. Права доступа могут относиться как к физическому, так и к программному обеспечению. В физическом смысле это относится к разным сотрудникам, которые должны получить физический доступ к определенным областям. Например, доступ в комнату, содержащую базовый блок, может быть ограничен операторами. Права на программное обеспечение относятся к уровню доступа различных пользователей к различным уровням данных и информации.

Политики паролей. Политики паролей относятся к руководствам или требованиям, касающимся структуры и использования паролей. Они могут потребоваться для доступа к компьютерной системе или группе файлов или отдельному файлу.

Шифрование данных. данные должны быть зашифрованы. Шифрование шифрует данные и делает их неразборчивыми без использования ключа. Ключ используется для расшифровки данных.

Антивирусное программное обеспечение. Антивирусное программное обеспечение сканирует файлы на наличие фрагментов кода, называемых сигнатурами, которые оно распознает как часть вируса. Обновление антивирусного программного обеспечения в основном включает обновление файла сигнатур. Это должно быть сделано настолько часто, насколько это возможно. Это даже больше в том случае, когда вы регулярно получаете файлы из внешних источников. Сама антивирусная программа будет время от времени обновляться. Эти обновления будут включать дополнительные функции и улучшенные методы сканирования. Важно помнить, что ни одно антивирусное программное обеспечение не является идеальным. Это только так хорошо, как методы, которые он использует для обнаружения вирусов и валюты файла подписи. Всегда есть вероятность того, что вирус останется незамеченным. Тем не менее, хорошая антивирусная система, установленная в вашей системе, очень важна и обычно обнаруживает большинство вирусов. При обнаружении вируса программное обеспечение попытка удалить вирус. Это называется очистка или дезинфекция. Иногда случается, что система может обнаружить вирус, но не избавиться от него. В этом случае вам обычно будет предоставлена возможность удаления или помещения в карантин зараженного файла. Когда файл помещается на карантин, он становится непригодным для использования и поэтому не может распространять вирус. Будущее обновление программного обеспечения может удалить вирус.

Практика трудоустройства персонала. Основой хорошей безопасности компании являются сотрудники, те, которые верные и заслуживающие доверия. Если сотрудники, вероятно, будут иметь доступ к конфиденциальной информации, они должны быть тщательно проверены, прежде чем они будут наняты. Чем чувствительнее информация, к которой у них есть доступ, тем важнее этот процесс. Продвижение на более чувствительные позиции может быть основано на хорошей истории или верности и доверии. Часть процесса ознакомления персонала и непрерывного обучения персонала должна прививать персоналу важность безопасности и осведомленность о последствиях ее нарушения.

Процедуры безопасности. Информация должна быть классифицирована на основе ее чувствительности. Права доступа к этой информации должны быть ограничены теми, кто должен знать. Для доступа к определенной информации сотруднику может потребоваться специальное разрешение на безопасность. Весь доступ к конфиденциальной информации должен быть зарегистрирован. Если конфиденциальная информация хранится в виде бумажных файлов, они должны храниться в надежном хранилище. Должны существовать процедуры, позволяющие сотрудникам сообщать о нарушениях или предполагаемых нарушениях безопасности. Они должны иметь возможность сообщать об этом, не опасаясь репрессий. В крупных организациях отделы безопасности могут быть созданы специально с целью обеспечения. Это часто делается в сочетании с судебной проверкой. Это особая форма аудита для выявления злоупотреблений и коррупции.

Ниже в таблице 1 приведены среднее арифметическое, стандартное отклонение и использование современных приложений безопасности в банках и АИС, что положительно отражается на банках и АИС, в частности[15]:

Таблица 1. показывает среднее арифметическое, стандартное отклонение и использование современных приложений безопасности в банках и АИС

Пункты	Арифмет	Среднеквад-	%	Масса

	ическое значение	ратичное отклонение		
Банк использует современные методы безопасности в планирование информационных систем учета	4.25	0.68	84.9	1
Банк использует современные методы безопасности в учет о информационных системах безопасности	4.10	0.73	81.9	6
Банк использует современные методы обеспечения безопасности для мониторинга производительности учетных информационных систем	4.12	0.7	82.3	4
Банк использует современные методы обеспечения безопасности для разработки применяемых в нем учетных информационных систем.	4.05	0.9	80.9	10
Банк имеет хорошую программу обучения безопасности информационных систем для своих пользователей.	4.07	0.92	81.3	9
Банк располагает современными учетными информационными системами, обеспечивающими хорошую кредитную защиту путем определения подходящего потолка для кредита	4.09	0.69	81.7	7
У вас есть хорошая программа безопасности информационных систем банка	3.85	1.08	76.9	12
Наибольшее количество атак на банки и бухгалтерские информационные системы приходится на компьютерные вирусные атаки.	4.11	0.86	83	5
Наибольшее количество атак на банки и бухгалтерские информационные системы совершаются путем прямых манипуляций.	4.08	0.79	81.5	8
Наибольшее количество атак на банки и бухгалтерские информационные системы приходится на несанкционированный доступ	4.02	0.85	80.3	11
Банки и бухгалтерские информационные системы имеют недостатки как системы	4.15	0.84	82.9	3

Обучение современным приложениям безопасности достаточно, чтобы получить необходимые знания	3.59	0.95	71.7	13
В общем	4.04	0.83	80.7	

В результате исследования были получены следующие результаты:

1. Банки используют современные методы обеспечения безопасности приложений в учетных информационных системах.
2. Существуют трудности в использовании информационных систем, бухгалтерского учета или их части.
3. Существуют трудности при использовании современных методов обеспечения безопасности приложений или их части.
4. Отсутствуют учетные информационные системы, используемые банками.
5. Периоды обучения и методы недостаточны для того, чтобы сотрудники могли предоставить им необходимые знания о современных приложениях безопасности.

3.3. Обеспечение информационной безопасности в экономических системах

Информационная безопасность является основной проблемой при использовании интернета и имеет первостепенное значение в экономическом секторе. В этом исследовании подчеркиваются растущие риски и угрозы безопасности, с которыми сталкивается финансовый сектор, поскольку возросший спрос на безопасность в банковском секторе порождает новые возможности для бизнеса, а также проблемы.

Высокий уровень информационной безопасности в секторе банковских и финансовых услуг может быть достигнут путем стремления к достижению целостности, конфиденциальности, доступности, гарантии и подотчетности. Оценка рисков информационной безопасности, стратегия, контроль реализации, мониторинг процесса и обновление помогают в достижении этих целей.

Security Scorecard проанализировала и оценила состояние безопасности почти 3000 финансовых учреждений, чтобы найти существующие уязвимости в банках, инвестиционных фирмах и других финансовых организациях для определения эффективности кибербезопасности финансового сектора. Разбивка данных по категориям безопасности, а также более внимательное рассмотрение показателей деятельности банков, застрахованных в FDIC, позволили выявить следующие ключевые аспекты финансового сектора:

В период с марта по август 2017 года у 45% финансовых компаний было по крайней мере одно вредоносное событие, что является доказательством того, что хакеры часто атакуют финансовую индустрию.

Финансовые учреждения становятся жертвами нарушений больше, чем компании в телекоммуникационном, транспортном, пищевом, производственном и фармацевтическом секторах вместе взятые.

Финансовая индустрия сталкивается с трудностями при управлении сторонними рисками безопасности, которые возникают из-за утечки учетных данных и паролей.

Что касается здоровья в области кибербезопасности, только 25 процентов из 20 самых высокоэффективных банков, застрахованных в FDIC, получили оценку A в DNS Health.

I. Внутренние угрозы

Беспечность персонала

Неосторожность конечного пользователя представляет собой самую большую угрозу безопасности для организаций, превосходя постоянную опасность, создаваемую вредоносными программами или организованными хакерскими атаками.

Внутреннее мошенничество и кража

Мошенничество с сотрудниками является одним из самых дорогих обязательств организации.

Одной из часто цитируемых статистических данных является ACFE (Ассоциация сертифицированных экспертиз по мошенничеству), которая из года в год сообщает, что компании теряют в среднем пять процентов доходов от мошенничества со стороны сотрудников.

На приведенной диаграмме 4 представлены лишь некоторые типологии внутреннего мошенничества, с которыми в настоящее время сталкиваются группы информационной безопасности в банковском секторе: кража со стороны клиентов, злоупотребление кредитами, нарушения политики, отмывание денег, мошенничество с закупками, мошенничество в торговле, расходы и платежная ведомость, а также кража данных.

Как финансовые организации должны реагировать на внутренние угрозы?

Внутренние политики и процессы

С самого начала целесообразно создать четко определенные политики и процессы, которые послужат общей отправной точкой для всей команды. Когда все сделано правильно и тщательно, эти документы проложат четкий путь к обеспечению единообразия и последовательности в методах и процессах, принятых при запуске.

Диаграмма 4. Типологии внутреннего мошенничества

Обучение персонала и проверка данных

Финансовые организации должны привлекать своих сотрудников к ответственности за коллективную безопасность компании. Настаивайте на том, что команда информационной безопасности не несет единоличную ответственность за безопасность - мы все владеем ею. Обучение осведомленности о безопасности должно дать сотрудникам возможность поступать правильно, когда они сталкиваются с событиями безопасности.

С другой стороны, что неудивительно, проверка данных при проверке потенциальных сотрудников является обязательной для всех банков.

Меры физической безопасности в дата-центрах

Крайне важно, чтобы вы защищали конфиденциальную информацию от физической кражи, физического повреждения данных и человеческих ошибок. Всегда необходимо уделять больше внимания физической безопасности в центрах обработки данных с постоянно растущей сложностью методов социальной инженерии и взлома.

Само собой разумеется, что центры обработки данных также должны быть защищены от стихийных бедствий, скачков напряжения, утечки воды, влажности, высокой температуры, пожара и т. д. Все это подпадает под физическую безопасность и контроль окружающей среды в центрах обработки данных.

Аутентификация и авторизация пользователя

Понимание конкретных проблем, связанных с доступом, а также разработка, развертывание и поддержание успешного контроля доступа для решения этих задач является важной частью мер безопасности для банков и организаций, оказывающих финансовые услуги. Это также одна из самых сложных задач.

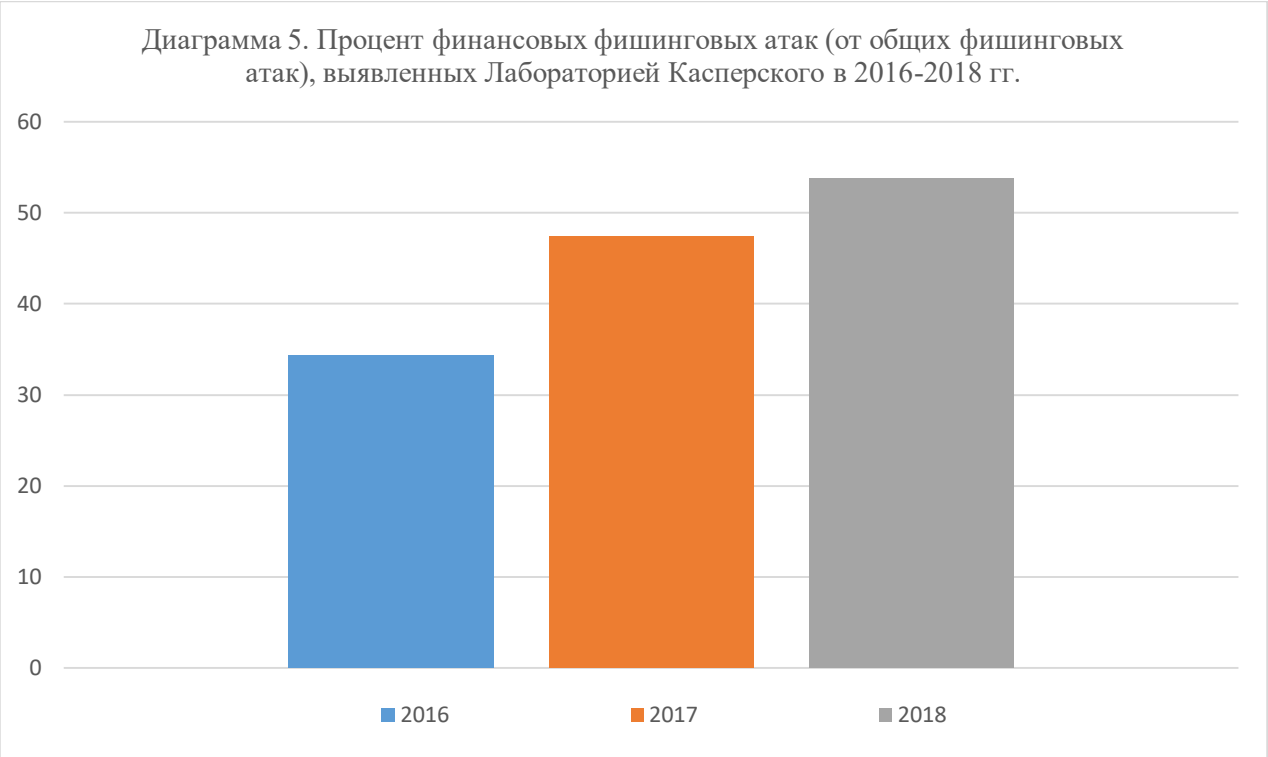
II. Внешние угрозы

Взлом

Онлайн-банкинг делает жизнь намного удобнее, но он также открывает ваши финансы для взломов. Важно предпринять активные шаги для защиты вашей организации от взлома данных, взломов и других методов использования информации об учетных записях, таких как фишинг, трояны, перехват сеансов и т. д. (Диаграмма 5.).

Атаки на клиентов

Банки, финансовые учреждения, поставщики, продавцы и все организации, занимающиеся онлайн-продажей товаров, обнаруживают растущую потребность в обеспечении безопасности своих транзакций. Для их клиентов одинаково важно обеспечить безопасность своего оборудования. Хакеры, как и все другие хищники, нападут на самую слабую добычу.



Новые угрозы

Мы живем в чрезвычайно захватывающее время, когда технологии стремительно развиваются на наших глазах, но мы знаем, что новые возможности для потребителей могут также предоставить новые возможности для хакеров и киберпреступников. Работая над информационной безопасностью и кибербезопасностью в банковском или любом другом секторе, очень важно использовать жизненно важные ресурсы, которые помогают нам оставаться на шаг впереди хакеров (Таблица 2).

Таблица 2. Типы угроз.

Общие Атаки На Стороне Клиента	**Нападения На Финансовые Системы**
➢ мошенничество с кредитными картами	➢ разрушающие / DDOS
➢ финансовые трояны	➢ шантажирование
➢ социальная инженерия	➢ Bank2Bank Мошенничество
➢ мобильное мошенничество	➢ ATM / POS-атаки

➢ фишинг	➢ Общие Атаки

Как финансовые организации должны реагировать на внешние угрозы?

Охрана периметра в банковском секторе

Являясь первой линией защиты от вторжений и нарушений безопасности, эффективная защита периметра должна стать неотъемлемым элементом стратегии безопасности для организаций, оказывающих финансовые услуги. Сочетание технологии, физической безопасности и развертывания обученного персонала часто является наиболее эффективным методом интеграции безопасности, создавая несколько уровней защиты для защиты периметра организации.

Аутентификация и авторизация пользователя

Повышение безопасности учетной записи довольно сложно, и в то же время упрощение работы с цифровыми данными для клиентов. Но онлайн-безопасность должна начинаться с процесса аутентификации. Требуется подтвердить, что пользователь является авторизованным пользователем, а не хакером или похитителем личных данных. Аутентификация обычно включает в себя одну многофакторную аутентификацию, а также дополнительные меры многоуровневой безопасности, когда это необходимо[25].

Управление патчами

Необходимо разработать процесс управления исправлениями, чтобы обеспечить принятие надлежащих превентивных мер против потенциальных угроз. Патчи применяются ко многим различным частям банковской информационной системы, которые включают операционные системы, серверы, маршрутизаторы, настольные компьютеры, почтовые клиенты, мобильные устройства, брандмауэры и многие другие компоненты, существующие в сетевой инфраструктуре.

Обучение клиентов

Обучение клиентов, несомненно, является одной из важных мер предосторожности, необходимых для защиты конфиденциальной информации клиентов и предоставления клиентам профессионального руководства о том, как защитить себя от кражи идентификационных данных, электронного мошенничества и других угроз, с которыми они могут столкнуться во время онлайн-банкинга.

Новые услуги для клиентов

Предлагая клиентам удобные способы ведения своих банковских дел при одновременном поддержании адекватных мер безопасности, чтобы защитить себя и свою клиентскую базу.

Работа с третьими сторонами для улучшения контроля

Работа со сторонними специалистами по кибербезопасности, безусловно, является разумным способом оптимизации бизнес-процессов и снижения затрат при оптимизации защиты. Кроме того, услуги, предоставляемые сторонним источником, освободят внутреннюю кибербезопасность и ИТ-персонал, чтобы они могли сосредоточиться на общих операциях и обеспечивать высочайший уровень обслуживания для вашей организации и ее клиентов. Но должная осмотрительность крайне важна для обеспечения выбора наилучших возможных партнеров, поскольку при аутсорсинге всегда существует риск увеличения рисков безопасности.

Многофакторная аутентификация

Методы аутентификации, которые зависят от более чем одного фактора, сложнее поставить под угрозу, чем однофакторные методы. Соответственно, правильно разработанные и реализованные методы многофакторной аутентификации являются более надежным и более сильным сдерживающим фактором, чем устаревшая однофакторная аутентификация по имени пользователя и паролю, и крайне важно, чтобы банки и другие финансовые

организации предприняли шаги для реализации безопасной многофакторной аутентификации.

Риски в банковской сфере, с которыми сталкивается каждый банк

После того, как мы определили угрозы, которые могут представлять риск для банковского сектора, следующим шагом будет выявление соответствующих слабых сторон (или уязвимостей) в ваших организационных системах, ресурсах, процессах или политиках, которые могут быть использованы угрозой.

Вот список рисков, с которыми постоянно сталкиваются банки, которые могут оказать потенциально неблагоприятное влияние на их бизнес.

- Кредитные риски
- Соблюденческий и правовой риск
- Операционный риск
- Процентная ставка и рыночный риск
- Риск ликвидности
- Стратегический риск
- Систематический риск
- Моральный ущерб
- Деловой риск

Вот наиболее распространенные типы атак, о которых сообщают компании, предоставляющие финансовые услуги:

- 43% несанкционированный доступ
- 32% вредоносный код
- 18% устойчивый зонд / сканирование
- 5% подозрительная активность
- 3% доступ или злоупотребление учетными данными

Также важно отметить, что 60% злоумышленников были идентифицированы как инсайдеры с доступом к сети, 44,5% имеют явное злонамеренное намерение и 15,5% вызывают события в результате непреднамеренных действий.

Индустрия финансовых услуг реагирует конкретными новыми стратегиями по снижению своих цифровых рисков. Результаты:

- 52% респондентов в опросе Global State of Information Security (GSIS) сообщили, что они используют управляемые службы безопасности для таких решений, как аутентификация, мониторинг и аналитика в реальном времени.
- 53% планируют потратить больше на улучшение безопасности сети и мобильных устройств
- 62% сейчас требуют, чтобы сотрудники проходили постоянное обучение по кибербезопасности

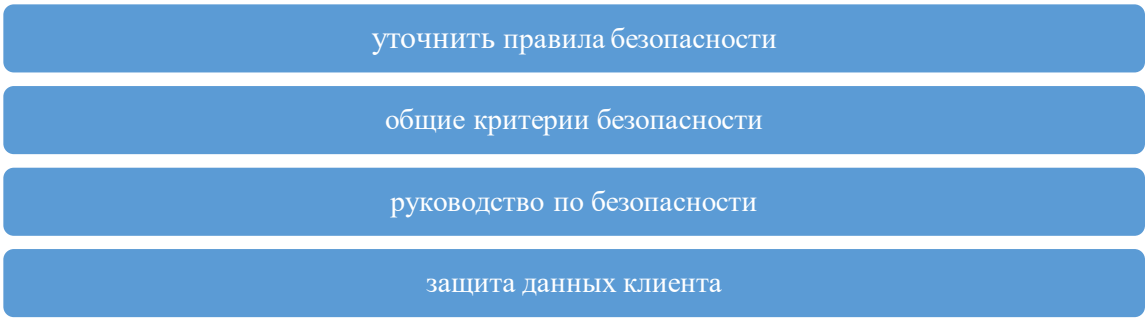
Рекомендации по повышению безопасности в банковской сфере

На основании собранной информации и упомянутого ряда желательных мер, стандартов и целей можно сформулировать в области информационной безопасности в банковском секторе:

Стандарт информационной безопасности. По словам участников отрасли, международные стандарты обычно служат ориентиром для реализации комплексной программы информационной безопасности, которая интегрирована в структуру управления рисками предприятия, соответствует нормативным требованиям и основана на последних отраслевых стандартах безопасности Технология может оказаться ценным союзником в этом начинании, объединяя сведения о рисках и угрозах по всему предприятию и превращая их в идеи, необходимые организациям для защиты своих активов и защиты своего бренда.

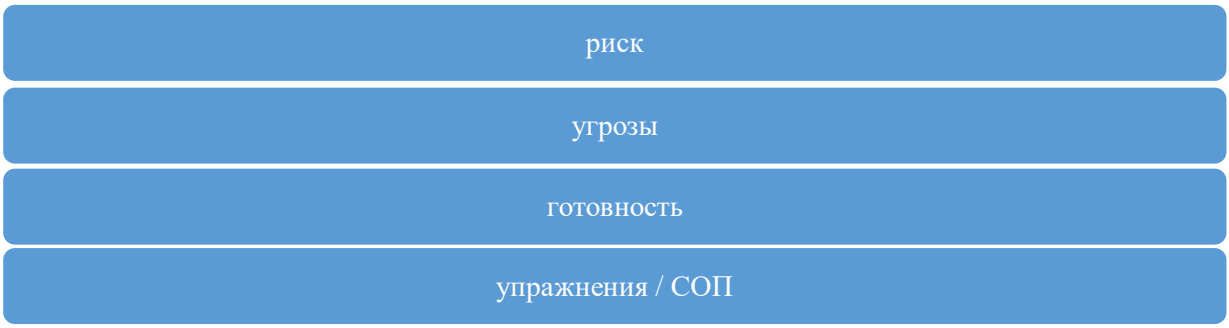
На Диаграмме 6. ниже показаны основные преимущества применения стандарта ISO / IEC 27001: 2012.

Диаграмма 6. основные преимущества применения стандарта ISO / IEC 27001: 2013.



Аналитика безопасности: сотрудничая друг с другом, международные поставщики финансовых услуг могут разработать набор общих индикаторов, которые помогут не только создать согласованные и сложные технические рекомендации, но и разработать соответствующий дружественный для оператора подход к реалистичным мерам безопасности.

Диаграмма 7. основные преимущества международного сотрудничества операторов финансового сектора.



На Диаграмме выше показаны основные преимущества международного сотрудничества операторов финансового сектора.

В методах защиты от вирусов имеются два направления:

1. Использование специфических программ-анализаторов, исполняющих беспрерывный контроль происхождения отклонений в деятельности практических программ, периодическую проверку присутствия других вероятных следов вирусной активности (например,

обнаружение нарушений цельности программного обеспечения), и входной контроль свежих программ перед их применением (по отличительным признакам присутствия в их теле вирусных образований).

2. Защита от неразрешенного копирования и распространения программ и значимой компьютерной информации является независимым видом защиты материальных прав, ориентированных на вопрос защиты интеллектуальной собственности, выраженной в форме программ ПЭВМ и значимых баз данных. Данная защита естественно осуществляется с помощью специфических программных средств, подвергающих защищаемые программы и информационной базы заблаговременной отделке (вставка парольной защиты, проверок по обращению к приспособлениям хранения ключа и основным дискетам, блокировка отладочных прерываний, контроль рабочей ПЭВМ по ее уникальным данным и т. д.), что приводит воспроизводимый код защищаемой программы и базы данных в состояние, мешающее его осуществлению на чужих машинах. Для увеличения безопасности применяются дополнительные аппаратные установки (ключи), подключаемые к разъему принтера или к системной шине ПЭВМ, и кодирование файлов, хранящих исполняемый код программы. всеобщим качеством спец средств для защиты программ от неразрешенного копирования представляется ограниченная надежность этой защиты, потому что в конечном случае выполняемый код программы поступает на исполнение в основной процессор в открытом виде и может быть прослежен с поддержкой аппаратных отладчиков. Впрочем, такое обстоятельство не снимает потребительские особенности средств защиты до нуля, так как главной целью их применения является в большой степени затруднить, пусть хотя бы временно, вероятность неразрешенного копирования ценной информации. Контроль цельности программ проводится с помощью:

– внешних средств (программ контроля целостности);

– внутренних средств (встроенных в саму программу).

Контроль цельности программ внешними средствами выполняется при старте системы и состоит в сравнении контрольных сумм раздельных блоков программ с их эталонными суммами. Контроль возможно производить также при каждом запуске программы на выполнение.

Контроль единства программ внутренними средствами исполняется при каждом запуске программы на выполнение и состоит в сравнении контрольных сумм раздельных блоков программ с их эталонными суммами. Подобный контроль применяется в программах для внутреннего пользования. Одним из вероятных каналов неразрешенного доступа к информации представляется несанкционированное модифицирование прикладных и специальных программ нарушителем дабы извлечения секретной информации. Эти изменения могут преследовать цель изменения законов разделения доступа или обхода их либо компанию незаметного канала получения секретной информации непосредственно из прикладных программ. Одним из способов противодействия данному является способ контроля целостности базового программного обеспечения специфическими программами. Впрочем, данный метод недостаточен, потому что предполагают, что программы контроля цельности не имеют возможности быть подвергнуты изменению нарушителем. При защите коммерческой информации, в большинстве случаев, применяются всевозможные существующие средства и системы защиты данных от несанкционированного доступа, впрочем, в любом случае подобает реально оценивать значимость защищаемой информации и ущерб, который может нанести ее утрата.

ЗАКЛЮЧЕНИЕ

Информационная безопасность имеет решающее значение в организации. Вся информация, хранящаяся в организации, должна храниться в безопасности. Информационная безопасность будет определяться как защита данных от любых угроз вируса. Информационная безопасность важна для организации, поскольку она может защищать конфиденциальную информацию, обеспечивает функцию организации, а также обеспечивает безопасную работу приложения, внедренного в систему информационных технологий организации, и информация является активом для организации. Даже несмотря на то, что информация важна для организации, существует несколько проблем для защиты информации и управления ею. Одной из проблем, с которыми сталкиваются в организации, является отсутствие понимания важности информационной безопасности. Когда сотрудникам не хватает знаний в области информационной безопасности с точки зрения сохранения их информации, организация легко подвергается атакам хакеров или другим угрозам, которые пытаются украсть или получить конфиденциальную информацию организации. Поэтому для всех сотрудников организации крайне важно иметь знания и понимание важности практики обеспечения информационной безопасности в организации для защиты конфиденциальных данных.

Простых инвестиций в информационную безопасность и технологии недостаточно. Он должен быть дополнен общеорганизационным обучением в отношении правил, стандартов, ценности данных и процессов для безопасного управления конфиденциальными данными.

Только путем надлежащего обучения и распространения знаний поставщики финансовых услуг могут сформулировать единый подход к управлению конфиденциальными данными и придерживаться регулирования в ближайшем будущем для борьбы с финансовой

киберпреступностью и повышения безопасности в банковских и финансовых учреждениях.

Ввиду эскалации угроз кибербезопасности, нацеленных на сектор высшего образования, обязательно, чтобы каждый пользователь и владелец ИТ-ресурса использовал соответствующую защиту кибербезопасности. Чтобы найти баланс между открытостью и контролем, а также затратами и выгодами, наиболее эффективным является использование подхода кибербезопасности, основанного на оценке риска. Такой подход проявляется в классификации ИТ-ресурсов, включая данные, системы приложений, конечные точки, серверы и сети, которые также делятся на 3 категории риска, а именно: высокий риск, средний риск и низкий риск, в зависимости от фактической цели использования.

В организации информация является важным бизнес-активом и необходима для бизнеса и поэтому нуждается в соответствующей защите. Это особенно важно в бизнес-среде, которая становится все более взаимосвязанной, в которой информация в настоящее время подвергается растущему числу и более широкому спектру угроз и уязвимостей. Повреждения, такие как вредоносный код, взлом компьютеров и атаки типа отказ в обслуживании, стали более распространенными, амбициозными и более изощренными. Таким образом, благодаря внедрению информационной безопасности в организации, она может защитить технологические активы, используемые в организации.

С точки зрения защиты функциональности организации, как общее руководство, так и руководство ИТ отвечают за реализацию информационной безопасности, которая защищает способность организации функционировать. Информация является наиболее важным элементом в организации для ведения бизнеса. Кроме того, организация хранит информацию о своих клиентах, поэтому для них крайне важно защитить информацию. Без информации бизнес невозможно вести.

Защищенным хранилищем информации; это может также позволить организации вести бизнес. Вот почему информационная безопасность важна в организациях.

ЛИТЕРАТУРА

1. Юрий Родичев (2016), Нормативная база и стандарты в области информационой безопасности, Питер, 257 с.
2. Е. Баранова, А. Бабаш (2015), Информационная безопасность и защита информаци, РИОР Инфра-М.
3. Валерй Бондарев (2017), Введение в информационную безопасность автоматизированых систем, МГТУ им. Н. Э. Бамана.
4. В. В. Ерохн (2015), Безопасность информационых систем, Флинт, 182 с.
5. Джон Эриксон(2017), Хакинг. Искусство эксплойта, Питер.
6. Козлов Сергеи, Защита информации. Устройства несанкционированного съема информации и борьба с ними, Трикста.
7. Макл Сикорски, Эндрю Хониг, Вскрытие покажет. Практический анализ вредоносного ПО, Питер
8. Райитман М., Искусство легального, анонимного и безопасного доступа к ресурсам Интернета, БХВ-Петербург.
9. Валерий Бондарев (2016), Анализ защищенности и мониторинг компьютерных сетей.
10. Нкита Скабцов, Аудит безопасности информационых систем, Питер, 269 с.
11. Владимир Фомичв, Дмитрий Мельников (2015), Криптографические методы защиты информаци. Издательство Юрайт,.
12. Андрей Бирюков (2018), Информационая безопасность: защита и нападение, ДМК-Пресс.
13. Бондайрев В., Введение в информационую безопасность автоматизированых систем,

14. Наталья Милославская, Михаил Сенаторов, Управление рисками информационой безопасиности, Горячая линия-Телеком.
15. С.П. Расторгуев, М.В. Литвиненко, Информационые операции в сети Интернет,.
16. Вадим Проскурн, Защита в операционых системах, Горячая линия-Телеком.
17. Bawaheh, Shasi S., Information security for Organizations and Accounting Information Siystems: A Jordan Banking Sector Case, International Review of Management and Business Research.
18. Garzian F., Handbok of Comunications Security, WIT Press Southampton, Boston.
19. Goryeva, Natalya, Luther, Elaine and Bromal, George, Exploring Acounting Information Systems and Embezlement from Nonprofit Originations, Issues in Information Systems.
20. Hal, James A., Acounting Information Systems, South-Western Cenga Learning.
21. Muhrtala, Tijani Oladipo and Ogunji, Mathias, Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies.
22. Neogy, Taposh Kumar, Evaluation of Eficiency of Acounting Information Systems: A Study on Mobile Telecomunication Companies in Bangladesh, Global Disclosure of Economics and Busines 2012.
23. Okpamen, Peter, Security of Information Systems in Organization: A Bank Model, Mediterranean Journal of Social Sciences, Published by MCSER-CEMAS- Sapienza University of Rome
24. Kieson, Donald B., Weygandt, Jerry J. and Warfield, Tery D., Intermediate Accounting, Sons, Incn.,
25. Spiceland, J. Davit, Sepe, Jaymes F., Nelson, Mark W. and Thomas, Wayne B.,

26. Intermediate Acounting, McGraw-Hil Education.
27. Varley, David, Concepts of Information Technology, Published by the ICDL Foundation, ICDL Module.
28. Zimerman, Markt Acceptable Use and Information Security Procedures, the Pennsylvania State University.

XÜLASƏ

Kiber məkanı və elektron rabitəni qorumaq dünya miqyasında bir hökumət və sənaye prioritetinə çevrilmişdir. İnformasiya və kommunikasiya texnologiyalarının iqtisadiyyatın ən vacib funksiyalarında artan əhəmiyyəti bütün sektorlarda, o cümlədən maliyyə sektorunda profilaktik və qoruyucu tədbirlərə ehtiyac yaradırdı.

Bu araşdırma, əksər ölkələrdə maliyyə sektorundakı məlumat təhlükəsizliyi öhdəliklərini sənaye perspektivləri ilə müqayisə etmək və gələcək prioritetlərin aydın görüntüsünü anlamaq, onları müqayisə etmək məqsədi daşıyır və tənzimləmə, sənaye prioritetləri arasındakı fərqləri anlamaq üçün məlumatlar uçotuna birləşdirilmiş bir yanaşmanı əhatə edir.

Açar sözlər: İnformasiya, Təhlükəsizlik, Şəbəkə, Kibertəhlükəsizlik

SUMMARY

Protecting cyberspace and electronic communications has become a global government and industry priority. The growing importance of information and communication technologies in the most important functions of the economy necessitated preventive and protective measures in all sectors, including the financial sector.

This study aims to compare information security commitments in the financial sector in most countries with industry perspectives and to understand a clear picture of future priorities, and includes an integrated approach to data accounting to understand the differences between regulation and industry priorities.

Keywords: Information, Security, Network, Cyber Security