Охрана предприятия

№3 (55), 2017

Оглавление

Книжное обозрение

Enterprise Risk Management: A Common Framework for the Entire Organization.

Безопасность в аэропорту. Охрана зоны общего пользования

Террористические акции в аэропортах Брюсселя и Стамбула вновь привлекли внимание экспертов к вопросам обеспечения безопасности в зоне (зале) общего пользования (до входа в так называемую «стерильную» зону). Именно там были совершены теракты в этих двух городах.

Этой проблеме посвящена статья в журнале Security Management (April, 2017). Автор публикации Скотт Стюарт считает, что простое увеличение числа охранников в зоне общего пользования (ЗОП) ничего не дает, кроме демонстрации силы для успокоения пассажиров и слабой надежды, что это отпугнет террористов. Распознать хорошо подготовленного террориста в толпе – задача не простая.

В некоторых аэропортах решили вынести первичную проверку багажа и пассажиров за пределы здания, на подходах к нему. Это, по мнению Стюарта, может быть эффективной мерой для небольших, местных аэропортов, но не для воздушных гаваней крупных мегаполисов с их гигантским пассажиропотоком. Важно иметь в виду, что задача террористов – поразить как можно больше людей. Поэтому организация первичного контроля за пределами здания мало что решает. У пунктов контроля так или иначе скапливается большое число людей и взрыв бомбы чреват значительными жертвами.

Тем не менее, у экспертов есть конкретные рекомендации по уменьшению связанных с терроризмом рисков.

Они уверены, что обычного, статичного контроля безопасности на входе в здание аэропорта (или на подходе) недостаточно. Необходимо организовать визуальное наблюдение на подступах, чтобы вычленить из потока людей, направляющихся в здание, подозрительные личности и проверить их до того, как они смешаются с плотной толпой на пункте контроля. Даже если террористы подорвут себя или откроют беспорядочную стрельбу, жертв будет меньше, чем внутри здания.

Многие международные аэропорты используют технологии, призванные распознать подозрительное поведение и сигнализировать дежурному оператору. Такая технология работает как на близких подступах к основному зданию, так и на прилегающих к аэропорту территориях.

Операторы, работающие с техникой сканирования носильных вещей и личного досмотра, как правило, не искушены в искусстве выявлять подозрительное поведение. То же самое можно сказать и про большинство охранников, приставленных к входным дверям. Эксперты советуют создавать группы специально обученных профессионалов,

способных своевременно выявить и отреагировать на неадекватное поведение возможных злоумышленников. Их место для работы – на подступах к аэропорту. Например, около ближайшей станции метро, автобусной остановки, паркинга...

Сочетание профессионалов визуального наблюдения, продвинутых технологий видеонаблюдения, адекватной коммуникации и координации с центром контроля за безопасностью повышает шансы на положительный результат.

Офицеры в штатском, работающие незаметно для окружающих, имеют перед террористами преимущество действовать первыми, застать их врасплох. Даже если и в этом случае не удастся полностью обезвредить террориста, инициатива лучше реагирования, риски массового поражения существенно ниже.

Тому имеются позитивные примеры. Так, в мае 2015 года в городе Гарланд (штат Техас) дорожная полиция предупредила местные власти о подозрительной машине, двигающейся в направлении аэропорта. Бдительные гаишники дали подробное описание внешности находившихся в автомобиле людей. Спецслужба, охраняющая аэропорт, успела подготовиться и обезвредить террористов.

По-новому думать и говорить о рисках

Мы все рабы собственных привычек. Поэтому время от времени важно вспоминать, что все в мире меняется и нам надо тоже меняться.

Таким философским заходом начинается статья в журнале Chief Security Officer (March 8, 2017), где слово предоставлено Стиву Гроссману, вице-президенту корпорации Bay Dynamics (специализируется на изучении и минимизации финансовых рисков). Он полагает, что тем, кто занимается вопросами корпоративной безопасности, полезно освежать свой подход к проблемам своей специальности. Прежде всего, освобождаться от «технологического» мышления. К сожалению, многие думают о безопасности в терминах технологий – сколько и какие межсетевые фильтры? Какие пакеты программных решений? Какие технологии СКУД? И так далее...

На самом деле защита предприятия представляет собой проблему управления рисками. В реальности инцидентов безопасности, в том числе атак хакеров, слишком много, чтобы успешно пытаться закрыть все уязвимости и прорехи. Как бы вы ни старались, какие совершенные технологии безопасности ни внедряли, угрозы и риски всегда остаются.

Поэтому необходимо находить новые подходы к проблеме корпоративной безопасности.

Как это делать, советует Стив Гроссман.

Изучайте и осваивайте само определение риска. Что собой представляет риск? Взаимодействие угрозы, уязвимости и воздействия (impact). Если в наличие нет ни одного из этих факторов, то нет и риска. Это вопрос приоритета. Многие пытаются устранить любую угрозу, залатать любую брешь. Это практически невозможно. Даже с финансовой точки зрения нецелесообразно. Просто не хватит никаких денег.

Следовательно, надо сосредоточить внимание на приоритетных направлениях защиты. Откуда исходят самые большие риски? Что и какими средствами защищать в первую очередь? Куда вкладывать ограниченные бюджетом деньги?

Фокусируйте первоочередное внимание на потенциальных последствиях для бизнеса. Какие области бизнеса, процессы понесут наибольшие потери в случае компрометации и нарушения нормальной работы компании. «Заточенным» на технику специалистам трудно сформировать общую картину рисков. Анализ только технических аспектов потенциальных угроз и уязвимостей мешает понять и оценить негативные последствия для бизнеса при реализации этих угроз. Именно конкретные результаты воздействия инцидентов безопасности на бизнес часто остаются за скобками анализа рисков.

Говорите в терминах рисков. Когда вы докладываете первым лицам компании, совету директоров о корпоративной безопасности, не следует подсчитывать количество уязвимостей и брешей, залатанных вами за отчетный период. Надо говорить о количестве рисков, которые удалось сократить. Без соответствующего контекста цифры проделанной работы мало о чем говорят. Если и говорить о цифрах, то о суммах денег, которые удалось сэкономить на минимизации рисков.

При принятии решений думайте о взаимосвязи угроз и уязвимостей в защите бизнеса. Там, где уязвимости не обнаружены, можно особенно не волноваться по поводу рисков. Конечно, речь не идет о том, что не надо выявлять и устранять уязвимости. Просто надо сосредоточить внимание на защите тех направлений, которые могут представлять для бизнеса наибольшую опасность в случае компрометации. К примеру, технологии предотвращения информационных утечек. Используйте их там, где хранятся наиболее важные, секретные данные. Задайте себе вопрос: что сегодня наиболее важно с точки зрения корпоративной безопасности? Ответ: то, что помогает избавиться или минимизировать наиболее опасные для бизнеса риски.

Оценивайте и измеряйте. Если вы не используете испытанные, проверенные метрики в оценке рисков и угроз, то можете пойти в неправильном направлении. Оценивать (и измерять) угрозы надо в контексте потенциальных негативных последствий для бизнеса.

12 вопросов соискателю вакансии по корпоративной безопасности

Джерри Бреннан предлагает дополнительные рекомендации для подготовки к собеседованию на предмет приема на работу офицером по безопасности (см. предыдущие выпуски нашего журнала). В этот раз он формулирует 12 наиболее вероятных вопросов, адресованные соискателю во время интервью.

1. Что вам известно о нашей компании и что вас в ней привлекает?

2. Почему вы заинтересованы в смене места работы?

3. На какую роль в деятельности компании вы рассчитываете?

4. Насколько ваш предшествующий опыт согласуется с этой ролью?

5. Расскажите о своей рабочей философии, о своем стиле работы, менеджмента?

6. Если спросить ваших прежних (или пока нынешних) начальников, как бы они описали ваши:
- Знания и способность продуцировать новые идеи
- Умение ладить и эффективно взаимодействовать с вышестоящими менеджерами
- Сильные стороны
- Слабые стороны или области, где вам еще надо подтянуться

7. Если спросить ваших коллег, что они могли бы сказать о совместной с вами работе?

8. С кем и какие проблемы во взаимоотношениях внутри коллектива у вас были, что вы делали для их решения?

9. Расскажите о ситуациях, где вы решали и действовали самостоятельно

10. Примеры, когда вы отбрасывали в сторону разногласия во имя дружной совместной работы

11. Случаются ошибки, вызывающие негативную реакцию руководства. Как вам удавалось сохранить хорошие рабочие отношения с начальством в таких случаях?

12. Какие у вас самого вопросы к нам?

(по материалам февральского номера журнала Security Magazine, 2017)

Основные угрозы для информационной безопасности в ближайшие три года

Форум информационной безопасности (Information Security Forum) выпустил исследование «Горизонт угроз». О его содержании и выводах пишет Тор Овалсруд в журнале Chief Information Officer.

В докладе отмечается, что сегодня организации полностью зависят от устойчивой и непрерывной соединяемости (connectivity) информационных систем управления, умных гаджетов, надежного персонала. Данная зависимость делает их весьма уязвимыми для хакерских атак на корпоративные сети и интернет инфраструктуру. Другая угроза – рост числа локальных и региональных конфликтов, чреватых потерями миллионов долларов для транснациональных корпораций.

В целях защиты организациям необходимо по новому взглянуть на модель безопасности, чья основная задача должна заключаться в обеспечении выживаемости бизнеса при хакерских атаках или стихийных бедствиях, угрожающих «соединяемости».

Форум рекомендует:

Владельцам и акционерам рассмотреть возможность резервирования альтернативных способов и путей коммуникации

Установить контакты с местными (региональными) администрациями для совместного формирования планов выживаемости бизнеса на случай обрушения интернета

Такие же деловые контакты необходимы и с производителями информационных технологий

Иметь под рукой план создания и использования альтернативных цепочек поставок в экстремальной ситуации

В докладе подробно характеризуется такое относительно новое направление киберкриминала как «информационный шантаж» (ransomware), когда хакеры, взламывая компьютерные сети, шифруют данные в базах и требуют выкупа за предоставление шифровальных ключей. Выплаты по этому виду преступлений в 2016 году возросли более чем вдвое по сравнению с 2015 годом. Эксперты прогнозируют резкий рост этих преступлений через взлом «интернета вещей» и последующее проникновение в корпоративные сети и базы данных.

Форум рекомендует:

Оказывать давление на производителей умных гаджетов, побуждая их совершенствовать защиту от хакеров

Контактировать с отраслевыми ассоциациями на предмет формирования минимальных стандартов безопасности информационных технологий

Установить достаточно высокие требования к безопасности приобретаемых информационных систем

Проводить с персоналом тренинги по безопасному использованию интернета вещей с использованием методов моделирования разных сценариев

Во взаимодействии с производителями и клиентами собирать разведданные о потенциальных угрозах, связанных с интернетом вещей.

Авторы исследования ожидают всплеск попыток криминала воздействовать на привилегированных пользователей интернета и корпоративные сети с целью получения доступа к критически важной информации (финансовые данные, интеллектуальная собственность, стратегические планы). Среди таких пользователей – не только представители топ-менеджмента, но также и их помощники, секретари, системные администраторы, инженеры по эксплуатации информационной инфраструктуры, даже внешние партнеры - подрядчики и поставщики. Не исключаются и попытки похищения членов семьи для шантажа и давления.

Эксперты рекомендуют:

Идентифицировать критически важные для бизнеса базы данных и тех из числа персонала, кто имеет к ним разрешенный доступ

Предусмотреть специальные меры защиты (в том числе и физической) привилегированных пользователей

Принять меры защиты от «инсайдеров» (регулярные проверки персонала, специально оговоренные условия работы в трудовых договорах и т.п.)

Вести мониторинг трафика в корпоративных сетях с выходом в интернет

Содействовать созданию в коллективе атмосферы доверия и одновременно бдительности.

Как бороться с криминалом в розничной торговле

Когда в конце нулевых годов кривая преступности в сфере розничной торговли США пошла резко вверх, все эксперты единодушно объясняли этот тренд экономическим кризисом. Но прошло почти 10 лет. Америка худо-бедно преодолевает кризис. Экономика медленно, но выздоравливает. Последние годы наметился устойчивый рост. А преступность в розничной торговле на убыль не идет. Напротив, из года в год ее уровень все выше. Из-за хищений, магазинных краж, разбойных нападений, ночных взломов американские ритейлеры в 2016 году потеряли по разным оценкам от 40 до 50 миллиардов долларов.

Говорит Рид Хейес, директор исследовательской организации Loss Prevention Research Council: «Последние два - три года наблюдается прямо-таки всплеск преступности в сфере торговли. И это при том, что ситуация в экономике страны явно изменилась к лучшему. Мы просто не знаем и не понимаем, почему уровень криминала все время растет» (Security Magazine, March, 2017).

Преступность в торговле не просто расширяется, но и ползет по вертикали, утверждает Том Михан, директор по безопасности и расследованиям корпорации Bloomingdale (сеть универмагов). Еще несколько лет назад криминал ориентировался на обычные лавки, магазины и аптеки. Сегодня он проявляется повсюду в розничной торговле, охватывает крупнейшие торговые сети. Причины этой тенденции Михану, как и Хейесу, не вполне ясны.

Магазинные кражи

По статистике их число ежегодно возрастает в соответствии с общей негативной тенденцией.

Loss Prevention Research Council (исследовательская организация по вопросам предотвращения потерь в торговле) рекомендует в качестве первого шага организовать торговый зал таким образом, чтобы преступнику было сложно совершить кражу. Т.е. товар должен быть физически защищен специальным барьером, стеклянной перегородкой, прочно зафиксирован на стенде.

В качестве второго шага рекомендуется максимально использовать все средства

охраны – от тревожной сигнализации до видеонаблюдения, включая соответствующую подготовку самих продавцов.

Наконец, следует иметь в виду и такие спецсредства как бирки, заполненные особыми чернилами, которые разрываются при попытке их снять ненадлежащим образом, или технологии, с помощью которых можно отслеживать, какое количество товара одномоменто снимается с полки. Некоторые ритейлеры используют специальные напольные плитки, фиксирующие, сколько времени проводит покупатель на одном месте: если больше обычного, поступает тревожный сигнал.

Многие научились правильно устанавливать камеры видеонаблюдения с технологией распознавания лица – на уровне головы среднестатистического человека. Такие видеокамеры наряду с ярким освещением, нарочито демонстрируемыми системами сигнализации могут отпугнуть, удержать преступников от попытки кражи.

Ограбления

Сеть аптек Walgreens стала внедрять специальные сейфовые шкафы, открывающиеся с задержкой по времени, давно известные в банках, но сравнительно новые в сфере розничной торговли. Здесь психологический расчет на то, что грабители нервничают и боятся любого промедления. Помимо этих сейфов служба безопасности Walgreens широко применяет средства световой и звуковой сигнализации на входе в аптеку, видеонаблюдение с архивацией данных. Эти охранные технологии афишируются через местные СМИ, дабы потенциальные злоумышленники имели представление о высоких рисках и трижды подумали, прежде чем решиться на ограбление.

Преступность охватила и многоканальные виды торговли. Например, когда товар заказывается по интернету, но приобретается в реальном магазине или доставляется на дом. Здесь для борьбы с кражами эффективны чипы радиочастотной идентификации, позволяющие проследить весь путь товара со склада к покупателю.

Минимизация рисков с помощью «сценарных» тренингов

Журнал Security Magazine (April, 2017) взял интервью у Брента О’Брайана, вице-президента по корпоративным тренингам корпорации Allied Universal, крупного игрока в охранной индустрии США.

Брент – ярый сторонник такого метода обучения и тренинга охранников как «сценарные игры». Поскольку работа охранника может быть сопряжена со смертельной опасностью, воссоздание в учебном классе или на полигоне как бы реальной ситуации – наилучший, по его мнению, способ научить офицеров и рядовых охранников действовать быстро, решительно и адекватно. Такие занятия помогают слушателям понять и осознать последствия неверных, ошибочных действий.

Кроме того, утверждает О’Брайан, «сценарные игры» позволяют вскрывать просчеты, уязвимости в системе охраны предприятия. «В ходе таких занятий преподаватели и слушатели могут обнаружить вещи, которые незаметны в повседневной рабочей

рутине. Здесь не только проверяются и развиваются профессиональные навыки, но одновременно подвергается испытанию, проверке эффективность действующей структуры охраны. К примеру, оценивается, насколько соответствуют имеющиеся в компании политики, инструкции, технологические и кадровые ресурсы потенциальным форс-мажорным ситуациям, которые могут возникнуть и потребовать максимально эффективного реагирования».

Содержание сценарных тренингов определяется спецификой индустрии. Для охраны высотных зданий ключевая тема – эвакуация людей при пожаре или террористической угрозе. В нефтехимической промышленности особое внимание на занятиях надо уделить охране здоровья персонала предприятия.

Но и внутри каждой отрасли бизнеса и экономики учеба охранников может быть разнообразной. Одни предпочитают теоретические тренинги в учебном классе, другие – практические занятия в реальной обстановке.

Так или иначе, симуляционные, приближенные к реальности тренинги предполагают определенный уровень квалификации участников. Иногда, говорит О'Брайан, приходится предварять практические занятия вводными учебными курсами, чтобы подровнять уровень базовых знаний слушателей, подготовить их к более сложным сценарным играм.

На такие тренинги приходят профессионалы с уже сложившимися взглядами на то, как надо действовать в той или иной ситуации. В ходе занятий, случается, они корректируют свои представления о работе.

Сценарные тренинги – обязательный компонент подготовки охранников для Seattle Children's Hospital, где проходят лечение дети с отклонением от нормы: аутентисты, душевнобольные, склонные к агрессии, самоубийству и т.п. Для службы безопасности больницы разработаны специальная инструкция поведения и специальная методология обучения. Все без исключения охранники, независимо от опыта и стажа работы, обязаны минимум раз в год проходить тренинги, где разыгрываются самые разные варианты непредсказуемого поведения больных детей, отрабатываются меры реагирования по «де-эскалации» форс-мажорных ситуаций.

Кроме того, тренинги предусматривают занятия по более широкой программе, охватывающей стандартные темы и вопросы, такие как эвакуация при пожаре, действия при попытке террористического захвата, меры защиты детей и персонала в случае стихийного бедствия и т.д.

«Число людей с ментальными, психическими заболеваниями - как взрослых, так и детей, постоянно растет, утверждает глава службы безопасности Seattle Children's Hospital Джим Сойер. Соответственно увеличивается и спрос на охранников со специальной подготовкой. Ключ к успеху – в регулярных, интенсивных тренингах, в ходе которых разыгрываются различные ситуации, до деталей отрабатываются приемы и способы решения возникающих проблем» (Security Magazine, April, 2017).

Как часто проводить аудит

кибербезопасности?

Эксперты отмечают острый дефицит специалистов по кибербезопасности в структуре отделов информационных технологий большинства организаций. Проверку состояния информзащиты там проводят обычно с привлечением внешних специалистов и не чаще одного раза в год. Достаточно ли это? Было достаточно 20-30 лет назад, но не сегодня, утверждает Дж. Грахис в мартовском выпуске журнала Chief Security Officer за 2017 год.

На фоне взрывообразного роста киберкриминала, пишет эксперт, у компаний нет другого выхода, кроме как проводить многоступенчатый, протяженный по времени аудит.

Сначала требуется сформировать план аудита на годовой период в зависимости от специфики бизнеса и приоритетов кибербезопасности. Например, организация определяет, что приоритетными для нее в данный момент являются риски, связанные с функционированием межсетевых экранов. Поэтому аудит начинается с тестирования firewalls.

В следующем месяце проверяется вторая по значению область инфраструктуры. К примеру, Active Directory (сервис, обеспечивающий наращиваемость и расширяемость компьютерной сети, а также функции распределения безопасности).

Затем настает очередь другого важного компонента, каковым могут быть мобильные устройства для служебного пользования, рабочие компьютерные станции, серверы, системы предотвращения несанкционированного вторжения, защиты электронной почты, антивирусы, веб-фильтры, приложения и прочие элементы компьютерной инфраструктуры, обладающие системами защиты.

Далее автор публикации излагает доводы в пользу фактически постоянного аудита кибербезопасности.

1. Такой вид киберпреступности как фишинг имеет целью установку в системе жертвы постоянного «зловреда». Статистика свидетельствует, что 30% фальшивых сообщений открываются по незнанию или утрате бдительности, вирусы внедряются в гаджеты, а затем незаметно вползают в корпоративные сети. Обнаружить их нелегко. Разовый годовой аудит может оказаться запоздалым и бесполезным средством обнаружения.

2. Зачастую уязвимости выявляются слишком поздно – по причине специфики рабочих процессов, отсутствия Patch Management System (системы управления «заплатами», которая автоматически проверяет наличие свежих обновлений и устанавливает их), некомпетентности обслуживающего персонала. Разовый аудит выявляет такие слабости с опозданием, чреватым серьезными угрозами для бизнеса.

3. По статистике компании Verizon, 63% информационных утечек обусловлены слабыми или украденными паролями. Важно регулярно, много чаще, чем раз в год, проверять эффективность используемых паролей, внедрять и поддерживать двухфакторную аутентификацию.

4. Корпоративные веб-сайты сегодня не статичны. Их контент постоянно обновляется. Посетители не ограничиваются чтением веб-страниц, но зачастую ведут

интерактивный диалог, отправляя на сайт запросы и прочую информацию, требующую соответствующей проверки на зловреды. Конечно, разовые годовые аудиты мало чем могут помочь в защите веб-сайтов, которая должна проверяться постоянно.

5. Невозможно обеспечить надежную защиту корпоративных данных, если вы не знаете, где она находится и, что самое главное, кто к ним имеет допуск. Защита эффективна тогда, когда проверка на доступ к базам данных проводится регулярно, а не раз в году!

В заключение автор подчеркивает высокую динамичность киберкриминала: каждый день в мире, где все связаны между собой интернетом в глобальном масштабе, появляются около 400 000 «зловредов». А между тем 70% мобильных дивайсов признаны уязвимыми для хакеров. И на этом фоне разовые ежегодные аудиты кибербезопасности представляются анахронизмом.

Охрана систем водоснабжения в США

Часть 2 Кибербезопасность

(начало см. в выпуске № 54)

Вопросами кибербезопасности компании водоснабжения серьезно занялись в конце нулевых годов, после ряда конкретных инцидентов из-за несостоявшегося работника, недобросовестного контрагента, других факторов риска.

Некто, раздраженный отказом принять его на работу, каким-то образом смог взломать внутренние компьютерные сети компании, нарушил работу запорно-регулирующих клапанов, что привело к несанкционированному сбросу отстойных вод. Никто из людей не пострадал, но был нанесен ущерб окружающим предприятие паркам и садам.

Проблемой для малых предприятий является приобретение и эксплуатация программных продуктов защиты от киберкриминала. По отдельности они не делают погоду на рынке подобных технологий. Производителям невыгодно учитывать специфику отдельных небольших предприятий.

Другой вызов заключается в распространении (равно как и в других отраслях бизнеса и экономики) такого вида криминала как кибершантаж. Взламываются базы данных, шифруются и затем следует ультиматум – платите за дешифровку. У небольших предприятий водоснабжения не хватает средств и технических навыков противостоять таким угрозам. Поэтому они вынуждены обращаться за помощью в государственные организации.

Многие владельцы и менеджеры начинают серьезно задумываться о потенциально негативных последствиях бесконтрольного пользования служащими компании т.н. «интернетом вещей». Эксплуатируемые там программные контроллеры, управляемые с помощью микропроцессоров, так или иначе, связаны с компьютерными сетями через интернет. И это – новые возможности для хакеров, активно использующих как фишинговые сообщения, так и внедрение вирусов и прочих «зловредов» напрямую в корпоративные сети.

Что могут противопоставить водоснабженческие компании? Межсетевые фильтры, детекторы вторжения извне, тренинг персонала.

Если крупные предприятия могут позволить себе иметь в штате профессионалов по информационной защите, то мелкие больше полагаются на аутсорсинг и помощь местных городских властей, заинтересованных в нормальном функционировании систем ЖКХ.

Руководители ряда городов создают и финансируют группы специалистов по кибербезопасности, которые плотно работают с предприятиями ЖКХ, энергообъектами, аэропортами и другими компонентами инфраструктуры, обеспечивающими нормальную жизнь населения.

Инсайдеры в банках – большая и недооцененная проблема

Еще продолжается расследование мошенничества в американском банке Wells Fargo. В течение ряда последних лет сотни служащих банка открывали неучтенные счета для клиентов, заработав на них миллионы долларов. Всего таких нелегальных счетов было создано ими с 2011 года порядка двух миллионов.

Мошеннические схемы раскрыты. Банк заплатит государству штраф в размере 185 миллионов долларов плюс 5 миллионов компенсации обманутым клиентам. Президент и одновременно генеральный директор банка Джон Стампф ушел в отставку. Сотни служащих уволены.

Журнал Security Management не оставил скандал без внимания, собрав мнения специалистов по безопасности в пространной публикации апрельского номера (2017 г.).

Эксперты обращают внимание на участившиеся случаи мошенничества в финансово-кредитной сфере. Преступления, совершаемые банковскими операционистами, занимают третье место в статистике утечек персональной и финансовой информации (на первом месте – внешние взломы, успешные из-за слабой информационной защиты, на втором – непредумышленные ошибки персонала).

Как отмечает генеральный прокурор Нью-Йорка Эрик Шнейдерман в интервью журналу Wall Street Journal, инсайдерство расцветает по причине невнимания банков к этой проблеме. Многие мошенничества можно было бы предотвратить, если бы банки тщательно отслеживали работу своих служащих, жестко контролировали счета, с которыми операционисты работают.

Эксперты выделяют несколько направлений, где проявляется деятельность инсайдеров.

Доступ к информации

Рост мошенничества в кредитно-финансовой сфере во многом связан с эволюцией

банковского дела под влиянием развития и внедрения информационных технологий. Движение денег в банках переходит из ручного режима в автоматический.

Соответственно, меняются и функции банковского операциониста. Финансовые трансакции проводятся с использованием персональной идентификационной информации, доступной банковскому служащему. Технологии облегчают операции с клиентскими счетами, но одновременно делают их весьма уязвимыми с точки зрения внутреннего криминала.

Развитие сети банкоматов и онлайн-банкинга сопровождается падением спроса на банковских кассиров. Категория банковских служащих по уровню легальных доходов скатилась вниз по сравнению с другими отраслями. В 2015 году средний доход банковских кассиров в США составлял чуть более 2 000 долларов в месяц - немного по нынешним американским меркам. Сравнительно низкие зарплаты, считают эксперты, объективно способствуют распространению мошеннических схем.

Хищение персональных данных и финансовой информации клиентов

Черный рынок персональных данных, информации о банковских счетах и картах процветает. Спрос на такую информацию из года в год везде растет. И это еще один фактор, побуждающий недобросовестных банковских служащих к совершению преступления. Налажено четкое взаимодействие между продавцами и покупателями. Компания Secure Banking Solution, которая специализируется на выпуске программных продуктов для банков, провела собственное расследование мошенничества в банке Midwestern bank. В ходе расследования установлено, что пара кассиров в течение года распечатывали ежедневно данные по 8 клиентским счетам и выносили на продажу, «зарабатывая» таким образом, по 200 долларов за каждый пакет информации.

Подобные схемы обнаруживаются и во время слияний и присоединений, когда часть служащих лишается работы. Это учитывается криминалом. Кевин Смит, в недавнем прошлом директор по безопасности Chevy Chase Bank, вспоминает о разоблачении работника колл-центра, который прямо на офисном паркинге продавал клиентскую информацию, Ему платили по 50 долларов за каждый пакет, включавший имя, адрес, номер телефона, дату рождения клиента.

Непродуманная система материального поощрения

Когда в Конгрессе США рассматривалось упомянутое в начале статьи скандальное дело Wells Fargo, законодатели обратили внимание на порочную, по их мнению, практику поощрения банковских служащих по числу открываемых ими клиентских счетов. Сами операционисты Wells Fargo жаловались на нереально завышенные требования по этим показателям со стороны начальства. Как отмечают эксперты, такая практика широко распространена среди банков. Причем за прибавление числа клиентов вознаграждаются не только рядовые служащие, но и руководители всех уровней. Таким образом, менеджеры охотно включаются в гонку за клиентами и уже меньше заинтересованы в жестком контроле за действиями своих подчиненных.

Как бороться с этим явлением? Эксперты рекомендуют проводить силами внешних независимых консультантов тщательные проверки работы служащих с клиентами.

(Продолжение в следующем номере нашего журнала)

Команда по оценке инсайдерских рисков. Кто в ней должен быть?

Эксперты уверены, что хотя внутренние инциденты безопасности, связанные с персоналом, случаются реже, чем внешние, урон от них многократно больше. По этой причине целесообразно в структуре компании иметь группу по оценке и изучению инсайдерских рисков, отмечает Райан Фрэнсис, ответственный редактор онлайнового журнала Chief Security Magazine (Febr. 27, 2017).

Автор публикации перечисляет, кем (и объясняет почему) должны комплектоваться такие группы внутри организации.

Представитель топ-менеджмента. Им может быть член совета директоров, гендиректор, замдиректора, акционер. Это нужно, чтобы, во-первых, «убедить» руководителей всех подразделений и направлений компании организовать у себя мониторинг инсайдерских рисков; во-вторых, определить строгие границы работы такой группы; в-третьих, связать ее работу со стратегическими целями, стоящими перед компанией.

Юрист. Определит соответствие внутреннего мониторинга местному и федеральному законодательствам. Юрист уточнит, что в работе персонала компании позволено контролировать: электронную переписку, посещение работниками веб-сайтов, пользование онлайновыми приложениями, что они выгружают из интернета и распечатывают. С другой стороны, к примеру, следить за личным онлайновым банкингом служащих чревато правовыми последствиями, если, не дай Бог, с его банковскими счетами случится что-то нехорошее.

Кадровик. Поможет документировать процесс мониторинга, проследить, не нарушаются ли права на личную жизнь (privacy). Участие кадровика необходимо хотя бы по той причине, что он/она располагает информацией о грядущих увольнениях (потенциальный риск), о финансовых или имущественных проблемах того или иного работника, что также заслуживает пристального внимания и расследования.

Системный администратор. Обеспечивает технологическую базу для мониторинга, помогает отслеживать и контролировать, кто и в каком объеме пользуется допуском к корпоративным базам данных.

Руководитель СБ. Он же должен и руководить командой.

Вопросы и области для внутреннего мониторинга:

Данные учетной записи (аккаунт) – имя пользователя и пароль, права и привилегии пользователя, допущенного в интернет и локальные сети (интранет)

Внешние аккаунты для клиентов, подрядчиков, консультантов, поставщиков и прочих партнеров, кому разрешен доступ в корпоративную сеть

Ограничения, установленные для использования в служебных целях личных компьютеров и мобильных устройств

Осведомленность персонала компании о политике и правилах безопасности

Система идентификации пользователей сети

Кадровые изменения – увольнения, приход новых сотрудников, перемещения по службе

Проявления агрессии и хулиганства на рабочих местах. Как с этим бороться

Термин «bullying» (хулиганство, задиристость, агрессивность, драчливость, дедовщина) в последнее время вошел в профессиональный словарь специалистов по корпоративной безопасности в США. Этому явлению посвящена публикация в журнале Security Magazine (апрельский номер за 2017 год).

По мнению экспертов из Института изучения вопросов хулиганства на работе (Workplace Bullying Institute), агрессивность отдельных служащих в отношении коллег обычно объясняется проявлением чувства собственной неполноценности, зависти, иногда – психическим заболеванием.

Социологические опросы в Великобритании, Канаде, Австралии, США и некоторых других западных странах дают такую цифру: каждый пятый рабочий или служащий подвергается на работе оскорблениям. И это проблема далеко не личностная. Она непосредственно влияет на результаты деятельности организации. Вот некоторые последствия:

- Высокая текучесть кадров
- Снижение производительности труда
- Потери в креативности, так как агрессии и травле чаще всего подвергаются более способные, талантливые работники
- Трудности с приглашением перспективных специалистов, если задета репутация компании.

Прямые и непрямые убытки от хулиганства и насилия, по некоторым подсчетам, уже обошлись США в 200 млрд долларов, Великобритании в 40 млрд. долларов.

Security Magazine рекомендует руководителям СБ во избежание или, по меньшей мере, минимизации последствий агрессии и хулиганства, придерживаться следующей стратегии:

- Стремиться расчленять агрессивно настроенные группы, не позволяя им консолидироваться и верховодить в коллективе компании.
- Быть в курсе того, что работники думают и говорят друг о друге.
- В то же время пресекать злобные сплетни, вызывающие напряженность во взаимоотношениях внутри коллектива.
- Немедленно расследовать все случаи агрессии и насилия.
- Сформировать эффективную систему информации о проявлениях хулиганства (поощрять доносительство).
- Оказывать моральную поддержку жертвам травли и агрессии.
- Если агрессивно ведет себя менеджер по отношению к подчиненным, то необходимо

обратиться за содействием к руководству компании.
- Если воспитательные и прочие паллиативные методы не помогают, добивайтесь увольнения хулиганов.

Несколько рекомендаций по защите налоговой информации работников компании

Хакеры охотятся за налоговой информацией для сбора компромата или поиска состоятельных жертв. Сэм Эллиот, директор управления по производству продуктов безопасности компании Bomgar, советует, как уберечь данные по налогам от преднамеренных утечек (csoonline.com, March, 14, 2017).

1. Обеспечьте защиту информации не только в период подготовки и предоставления налоговых деклараций, но в течение всего года, так как многие фишинговые схемы рассчитаны на длительный срок действия.

2. Не экономьте на инвестициях в шифрование и двухфакторную аутентификацию. Двухфакторные пароли существенно снижают риски от хакерских атак. Шифрование остается одним из самых надежных способов защитить персональные данные, содержащиеся в налоговых документах.

3. Осуществляйте регулярные аудиты. Визуальная недоступность (отсутствие visibility) является главной причиной неспособности обнаружить и своевременно отреагировать на утечку данных. Компании просто обязаны регулярно проверять протоколы доступа к сетям и базам данных. Особенно это касается отраслей и организаций с высоким уровнем сменяемости кадров. Нередко случается, что уволенный работник продолжает сохранять допуск к корпоративным сетям и базам данных. Аудиты протоколов обязательны в периоды подачи налоговых деклараций и после, в продолжение всего года. По меньшей мере, ежеквартально. Причем, это касается не только своего персонала, но и тех из партнеров и клиентов, кто пользуется постоянным или временным допуском. Регулярные аудиты помогают своевременно обнаруживать подозрительную активность в сетях, проводить расследование, минимизировать потери от утечек.

4. Обеспечьте защиту привилегированных пользователей. Множество крупных утечек обусловлены кражей или злоупотреблением привилегированных прав допуска. Компании обязаны следить, кто имеет привилегированный допуск к охраняемой информации, обращать внимание на избыточность допуска. Необходимо для каждого пользователя устанавливать индивидуальную конфигурацию доступа в зависимости от служебной необходимости.

5. Обучайте и тренируйте персонал. Все служащие должны знать о рисках и уязвимостях в работе с информацией, понимать, как надо действовать при обнаружении подозрительных e-mail или других признаках попыток взлома сетей. Важно разъяснять меры предосторожности при нахождении в социальных сетях. Регулярно проводите такие тренинги, формируйте культуру постоянной учебы во имя

безопасности компании, защиты бизнеса.

Управление рисками предприятия. Лучшие практики

В прошлом году Административно-бюджетное управление США призвало все федеральные ведомства осуществлять программу Управления рисками предприятия (ERM), чтобы эффективнее минимизировать риски и угрозы стратегическим целям и задачам. В результате в недрах американского правительства родился доклад «Управление рисками предприятия: опыт отдельных агентств демонстрирует лучшие практики в этой сфере».

Журнал Security Management ознакомился с докладом и, посчитав его весьма полезным для частных компаний, кратко процитировал 6 лучших компонентов (практик) успешного управления рисками.

1. Связь ERM со стратегическими целями и задачами предприятия

В этом случае обеспечивается поддержка и непосредственное участие в реализации программы ERM руководителей организации. Персонал организации воспринимает программу как важное направление деятельности компании.

2. Идентификация рисков

Успешные предприятия формируют культуру «информирования о рисках» (risk-informed), мотивирующую работников организации изучать потенциальные риски, свободно и открыто обсуждать эти вопросы с коллегами и руководством.

3. Анализ и оценка рисков

Успешные организации интегрируют программы по анализу и оценке рисков со стратегическим планированием, что, в частности, улучшает процессы планирования расходов, привлечения ресурсов на имплементацию этих программ.

4. Разработка мер по минимизации рисков

Важно, чтобы программы ERM учитывали специфику предприятий. В этом случае облегчается поиск и анализ рисков. Руководство выбирает такие меры по их минимизации, которые наилучшим образом соответствуют структуре и культуре организации.

5. Мониторинг рисков

Мониторинг рисков следует осуществлять постоянно. Регулярно докладывать о его результатах. Также необходимо отслеживать последствия предпринимаемых шагов по предотвращению или минимизации рисков, чтобы иметь четкое представление, насколько эти меры успешны и следует ли предпринимать дополнительные усилия.

6. Прозрачность ERM

Важно отладить систему ознакомления с процессами и результатами ERM как акционеров компании, так и регуляторов. Это необходимо для обеспечения поддержки программ ERM со стороны топ-менеджмента, владельцев компании, госорганов.

Охрана отелей. Опыт Marriott

Охрана гостиничного бизнеса сложна, так как требует правильного баланса между традицией гостеприимства и современным уровнем безопасности. Сочетать то и другое нелегко. Но это удается команде, возглавляемой Аланом Орлобом, вице-президентом по глобальной охране и безопасности Marriott International, транснациональной корпорации, обслуживающей 5 500 отелей более чем в 100 странах мира.

Огромное внимание в службе безопасности Marriott уделяется анализу обстановки в разных странах мира, разработке мер по обеспечению охраны отелей. В интервью журналу Security Magazine (March, 2017) Алан Орлоб рассказывает о работе созданной им группе аналитиков, внимание которых сфокусировано на отслеживании угроз по каждому из отелей сети Marriott.

Для каждого отеля определяется свой уровень необходимой охраны. Для одних – охранники на входе, регулярное патрулирование внутри, система электронных замков с дистанционным управлением. Для других – дополнительно металлодетекторы на каждом входе, рентген-сканеры, усиленное видеонаблюдение, фиксирующее и сигнализирующее о подозрительной активности внутри и вокруг отеля.

Конкретные рекомендации разрабатываются и предлагаются командой Орлоба, которая включает специалистов по тренингу. Последние проверяют на месте подготовку персонала к форс-мажорным ситуациям, уделяя особое внимание отелям в регионах и странах повышенного риска.

Орлоб подчеркивает огромное значение отношений с владельцами, акционерами отелей в каждой отдельно взятой стране (сеть Marriott занимает в основном управлением гостиничным хозяйством). Его задача – убеждать владельцев, что инвестиции в охрану и безопасность многократно оправдываются в острой конкурентной борьбе за клиентов. Репутация надежно охраняемого объекта не раз привлекала в отели Marriott множество клиентов в странах с нестабильной ситуацией.

Команда Орлоба систематически проводит тестирование охраны. Для этого приглашаются консультанты со стороны. Их задача – незаметно пронести сверток, предположительно с «взрывчаткой», совершить иное действие, создающее инцидент безопасности. Как утверждает Орлоб, такие проверки проводятся 2 или 3 раза в год по каждому из отелей сети Marriott. Результаты тестирования докладываются руководству корпорации.

Отель Marriott в Триполи (Ливия) открылся буквально за считанные недели до начала «арабской весны». И вскоре был закрыт из-за начавшейся гражданской войны и внешней агрессии. Владельцы отеля недавно обратились в службу безопасности корпорации с просьбой вновь его открыть. Проведенное группой Орлоба тщательное изучение обстановки в городе и стране с прогнозом развития событий показало, что

риски для гостей и персонала гостиницы остаются пока слишком большими. Было рекомендовано с открытием не торопиться.

Enterprise Risk Management: A Common Framework for the Entire Organization.

Enterprise Risk Management: A Common Framework for the Entire Organization.
By Phillip E.J. Green. Butterworth-Heinemann; Elsevier.com; 260 pages; $49.95.

Книга небезосновательно претендует на всеохватывающий взгляд на практику управления рисками. Раскрываются практически все сферы применения методологии ERM (управление рисками предприятия) – от физических (охрана здоровья, окружающая среда, операционные риски и т.п.) до виртуальных, связанных с кибербезопасностью.

Отдельные главы посвящены вопросам управления финансовыми рисками, глобальными и стратегическими, страховыми и другими рисками. Каждая глава книги предлагает дискуссию по конкретной теме, например, по рискам в сфере управления цепочками поставок.

Некоторые разделы представляют особый, повышенный интерес. К примеру, глава об инсайдерских рисках. Здесь дан глубокий анализ проблемы, единственный недостаток которого заключается в выводе автора, что все ошибочные действия инсайдеров носят злонамеренный характер, в то время как нередко они объясняются просто ошибками, недочетами работы. В этой же главе подробно разбирается такой вид криминала как фишинг.

Очень любопытна глава о формировании в компании культуры управления рисками. В частности, убедительно показывается, что стремление менеджмента контролировать некоторые виды рисков с помощью материального поощрения особо отличившихся служащих способно вызывать раздражение, склоки, недовольство в коллективе со всеми вытекающими возможными последствиями инсайдерства.

Книгу завершает реальная история возвышения и падения некогда крупнейшей в США сети видео проката Blockbuster. Причиной ее разорения, вытеснения с рынка более успешным конкурентом, компанией Netflix, стало неумелое, ошибочное осуществление программы ERM.

Глубокая по содержанию монография, возможно, создаст для слабо подготовленного читателя некоторые трудности в освоении материала, например, в главе, посвященной финансовым рискам. Тем не менее, эксперты настойчиво рекомендуют книгу самому широкому кругу специалистов в сфере индустрии безопасности.