Охрана предприятия

№2 (48), 2016

Главная тема

Что ожидает индустрию безопасности в 2016 году

Лидерство

Зачем организации нужен «главный специалист по управлению рисками»?

Новые технологии, методологии

Как формировать среду безопасности на этапе проектирования строительства зданий

Будущее за термальными камерами наблюдения

Безопасность органов судопроизводства требует хорошо налаженной координации

Инструкция по защите паролей

Как клиенты реагируют на утечки информации

Экономика и финансы

Как убедить финансового директора в необходимости инвестирования в службу безопасности компании

Риски и угрозы безопасности бизнеса

Банковский сектор: кибер-риски партнерства

Товарные потери увеличиваются

Системы контроля и управления допуском

На пути модернизации СКУД

Рекомендации специалиста

Как улучшить свое резюме

Пять наиболее распространенных ошибок реагирования на инцидент безопасности

Исследования

Насколько эффективны планы действий в чрезвычайной ситуации, принятые в американских университетах?

Книжное обозрение

A Law Enforcement and Security Officers' Guide to Responding to Bomb Threats Jim Smith; Reviewed by Hugh J. Martin

Что ожидает индустрию безопасности в 2016 году

Рядом соображений делится эксперт Тэйлор Амердинг в онлайновом издании Chief Security Officer.

• Прогнозирование инцидентов безопасности играет возрастающую роль, постепенно тесня на второй план технологии предотвращения и обнаружения (prevention, detection).

• Методы «беспаспортной» аутентификации получают преимущественное распространение. Это, в первую очередь, биометрия, геолокация, пиктография.

• В 2016 году, похоже, мир впервые столкнется с открыто объявленными кибервойнами со стороны хакеров, террористов и даже целых государств не ради наживы, а во имя геополитических целей. В числе первостепенных объектов нападения – критически важная инфраструктура, разрушение которой чревато огромными человеческими и материальными потерями.

• Хакеры уже не будут ограничиваться атаками на крупные организации, которые худо-бедно способны себя защитить. Собирая и анализируя большие массивы информации, киберпреступники расширяют для себя возможности нападения на средние и малые предприятия.

• Другая тенденция – все большее вовлечение в кибервойны развивающихся стран. Такие страны как, например, Нигерия, уже испытывают на себе разрушительные последствия мощных кибератак.

• «Интернет вещей» становится благоприятной средой для подготовки и осуществления хакерских нападений. Начиненные современными технологиями холодильники, машины по приготовлению кофе, автомобили, лечебное оборудование, разного рода мобильные устройства, которые могут себе позволить не бедные люди - лакомые цели для хакеров. Эти устройства, зачастую содержащие важную персональную информацию, как правило, не обладают надежной защитой от злоумышленников.

• На смену хакерам любителям, одиночкам приходят отлично организованные

гангстерские группы, которым доступны самые совершенные технологии взлома компьютеров и сетей. Что, в свою очередь, стимулирует производство и продажу не менее изощренных инструментов защиты от киберпреступников.

• Структура Интернета, как она сложилась за последние 20 лет, устаревает. Речь идет не только о «железе», но и о программном обеспечении. Выпускаются сотни и тысячи новых приложений, но очень часто на уже использовавшихся кодах, с теми же уязвимостями и слабостями. «Призраки» устаревшего интернета вновь будут нас посещать и пугать.

• Все больше организаций передают свои данные в «облачные» вычисления. Легко представить, что «плохие парни» пытаются находить и использовать лазейки для доступа к этой информации, прикрываясь легальными сетевыми ресурсами для проникновения в «облака».

• Неспособность многих организаций и даже стран воспитать достаточное число талантов в области информационной защиты, превращается в острейшую проблему. Некоторые эксперты полагают, что спрос на специалистов в этой сфере возрастет в ближайшие два года на 53%.

Зачем организации нужен «главный специалист по управлению рисками»?

Необходимость введения в штатное расписание должности главного специалиста по управлению рисками обусловлено, прежде всего, растущими день ото дня киберугрозами. Многие эксперты полагают, что такой специалист должен не только анализировать, отслеживать, оценивать, прогнозировать, устранять такие риски, но и обеспечивать соответствие внутренних инструкций часто меняющимся правилам и требованиями к безопасности со стороны регуляторов, контролировать их исполнение.

Амир Мизхар, эксперт по противодействию киберпреступности, на сайте securitymagazine.com называет шесть объективных причин, вызывающих необходимость появления в штатном расписании такой должности как «главный специалист по управлению рисками» (Chief Risk Officer).

1. Возрастающее давление регуляторов

В последнее время в большинстве стран и на международном уровне постоянно принимаются документы, регламентирующие деятельность компаний и организаций относительно киберугроз, вводящие новые, все более строгие стандарты работы с данными. В результате организации вынуждены регулярно вносить те или иные коррективы в свою работу, учитывая нововведения регуляторов. Именно главный специалист по управлению рисками должен следить за соответствием внутренних правил требованиям национальных и международных регуляторов, своевременно вносить коррективы.

2. Развитие каналов передачи корпоративных данных

Сегодня с распространением мобильных девайсов дистанционное соединение с

хранилищами данных вызвало к жизни новые и острые проблемы информационной защиты. Массовое увлечение социальными сетями породило еще одну реальную угрозу – непредумышленную утечку важной служебной информации. Позиция специалиста по рискам в организации – ключевая для выявления и минимизации таких угроз.

3. Мода на облачные вычисления

Зачастую компании слишком доверчиво относятся к передаче в «облака» информации и функций. Громкий скандал вокруг компрометации баз данных крупной торговой сети Target как раз связан с взломом «облачной» инфраструктуры. Опять же одна из ключевых задач специалиста по рискам – своевременно анализировать, идентифицировать и устранять «облачные» уязвимости.

4. Рост злоупотреблений внутри компаний

Угрозы приходят не только извне, но и внутри организаций. Согласно исследованиям в разных странах, компании ежегодно теряют до 5% своих доходов из-за хищений со стороны персонала. Особую опасность представляют потенциальные преступники из числа тех, кому по работе полагается знать пароли и коды, иметь доступ к финансовой информации. Например, пойманные за руку служащие банков, понимая, что незаконные трансакции привлекут внимание, обычно предпочитают воровать малыми суммами. Кто должен следить за этими преступлениями? Позиция специалиста по управлению рисками наилучшим образом подходит и здесь.

5. Создание новых рубежей информационной защиты

Роль специалиста по управлению рисками предполагает тесное взаимодействие с коллегами, партнерами, внешними экспертами на предмет разработки стратегии и тактики противодействия киберпреступности. Иметь в своем распоряжении рекомендации квалифицированных специалистов по разным аспектам кибербезопасности – значит уметь прогнозировать угрозы и их потенциальные последствия.

6. Многофункциональная безопасность

Сегодня бизнес вынужден вкладывать средства в приобретение различных программных приложений, рассчитанных по отдельности на защиту электронной почты, обмен файлами, мобильные средства связи, «облачных» вычислений… Главный специалист по управлению рисками должен координировать эту работу, стремясь к интеграции и унификации разных программных продуктов.

Как формировать среду безопасности на этапе проектирования строительства зданий

С. Людвиг, автор статьи на сайте csoonline.com (6 января 2016), упоминает метод, используемый в планировании безопасности, который опирается на особенности

окружающего ландшафта. Этот метод автор называет «Противодействие криминалу через дизайн среды» (Crime Prevention Through Environmental Design).

В статье рассматриваются основополагающие принципы методологии:

Прозрачность (обозримость, просматриваемость) окружающей территории

В темное время суток периметр и подходы к зданию должны быть хорошо освещены. Для этого рекомендуется устанавливать осветительные приборы каждые три метра. При этом важно учесть, чтобы разница между наиболее и наименее освещаемыми местами была минимальной. Предназначение системы освещения – фиксировать изнутри, кто подъезжает или подходит.

Во внимание принимается правило 3-7 футов. Оно означает, что все посадки по периметру (кроме деревьев) не должны превышать 3 фута (около метра). Что касается деревьев, то все листья необходимо удалять на высоте не менее 7 футов (чуть более 2 метров).

Эксперты отмечают, что строители нередко не обращают внимания на обозримость окружающего ландшафта. Если, к примеру, места для паркинга хорошо просматривается с любого этажа здания, то потенциальный преступник еще 100 раз подумает, стоит ли рисковать, залезая в чужой автомобиль.

Другой важный компонент проектирования с учетом безопасности – размеры и расположение окон. Желательно, чтобы окна были не зашторенными, свободными от горшков с цветами и других предметов.

Контроль доступа

Важно проектировать как можно меньше внешних дверей, самый наилучший с точки зрения охраны вариант – иметь только один подъезд. Конечно, такой подход обещает определенный дискомфорт. Но всегда требует ответа стоит вопрос о нахождении оптимального соотношения между удобством и безопасностью.

Другой существенный компонент – указатели, облегчающие нахождение нужной комнаты (помещения). Со временем здания старятся, требуют ремонта, перестройки, каких-то улучшений. В иных случаях департаменты занимающей здание организации часто меняют свое местоположения. Когда люди блуждают и подолгу не могут найти то, что ищут, создаются благоприятные условия для планирования и совершения преступления.

При проектировании новых зданий позитивное значение имеет правильное расположение внутренних помещений, облегчающее поиск нужной комнаты. Существенную роль играют и знаки, указатели. В некоторых американских госпиталях коридоры и холлы разрисованы линиями разного цвета, помогающими выбрать правильный маршрут.

Будущее за тепловизионными

камерами наблюдения

Одной тепловизионной камеры достаточно для слежения за ситуацией на пространстве, превышающем размеры футбольного поля. Кроме обнаружения объекта такая камера одновременно способна осуществлять его верификацию, независимо от того, интегрировано видеонаблюдение в сложную систему безопасности или работает на основе отдельного приложения.

Сфера применения тепловизионных камер наблюдения обширна – экономическая инфраструктура, нефтехимия, электросети, морские и воздушные порты, граница, коммерческие объекты... Они прекрасно зарекомендовали себя при охране крупных объектов, таких как нефтеперерабатывающие комплексы с периметром протяженностью более 10 миль. Оказались незаменимыми и в тесноте городов, к примеру, в системе обеспечения безопасности Международного торгового центра в Нью-Йорке.

В Австралии тепловизионные камеры отлично справляются с задачей слежения за распространением губительных пожаров, реагируя как на температуру, так и визуально - на сполохи огня.

Все большее распространение получают тепловизионные технологии в аэропортах, например, для определения пассажиров с высокой температурой, возвращающихся из стран высокого эпидемического риска (Эбола, Зика и пр.). Особый эффект дает сочетание реакции на температуру человеческого тела с тем, как выглядит пассажир. Интегрированные в традиционное видеонаблюдение, термальные камеры, конечно, не измеряют температуру подобно градуснику, но способны различить небольшие отклонения в излучении тепла в потоке людей.

Мобильность и гибкость – отличительные качества тепловизионных камер, что успешно используется в системах наблюдения движущихся объектов. Таких, например, как гигантский морской контейнеровоз «Беджамин Франклин», где камеры отслеживают весь периметр корабля на большую глубину, фиксируя все, что появляется в объективе камер, сопоставляя это с датчиками тепла в любое время суток. Эта технология отлично зарекомендовала себя при прохождении судов в районах, где промышляют сомалийские пираты.

Способность «видеть» в темноте, в условиях тумана, песчаной бури, сильного задымления используется на дронах, запускаемых как для военных, так и гражданских задач. Еще одна возможная функция – определять скорость движущегося объекта и посылать пользователям сигнал тревоги, когда она превышает установленный предел. Точно так же включается тревожная сигнализация, если тепловое излучение стороннего объекта выходит за рамки определенного пользователем диапазона температуры.

В последнее время производители предлагают тепловизионные камеры с целым набором функций:

- георегистрация, предусматривающая реагирование исключительно на появление в отслеживаемой зоне людей или других крупных объектов (при этом игнорируются мелкие животные, птицы, листопад);

- определение размеров, скорости и направления движения объекта.

Важное преимущество – незначительное потребление энергии, позволяющее использовать солнечные батареи и беспроводные опции энергообеспечения.

(по материалам журнала Security Magazine)

Безопасность органов судопроизводства требует хорошо налаженной координации

Тему охраны судебных органов затронула в журнале «Security Magazine» Клэр Мейер (декабрьский выпуск за 2015 год). В подготовке статьи ей помогал Стив Стэдмен, в прошлом руководитель службы безопасности верховного суда штата Висконсин (север США), а в настоящем – директор по вопросам охраны судебных органов компании Ralph L. Carr Justic Center в Денвере.

Одна из главных забот Стэдмена – укрепление внешнего периметра зданий, где проходят судебные процессы. В этом деле он опирается в первую очередь на современные технологии: магнитометры (приборы для измерения характеристик магнитного поля и магнитных свойств материалов), рентгенографическое оборудование (x-ray), тревожная сигнализация, видеонаблюдение с аналитическими функциями.

«Мы стремимся фиксировать угрозы уже на линии периметра охраняемой территории, не забывая о разных уровнях охраны внутри здания», - говорит эксперт. «Наша цель – обеспечить избыточную, с запасом, концентрацию охранного персонала и оборудования. То, что не заметит один, не уйдет от внимания другого».

Охрана периметра в общей системе безопасности, подчеркивает Стэдмен, играет первостепенную роль. Именно здесь, на передовой линии обороны, мы должны реагировать на попытки несанкционированного просачивания, обращать внимание на всяких праздношатающихся, на подозрительные предметы, потенциально представляющие опасность. Стэдмен работает над усовершенствованием технологий, над уменьшением числа ложных сигналов.

В фокусе его внимания и персонал охранников. Последние, правда, ему напрямую не подчиняются, так как охрану внутри зданий суда обычно выполняют полицейские. Однако, повседневная координация работы с окружными шерифами, с патрульной службой полиции штата – залог успеха. «В конечном счете, у нас одна цель, - подчеркивает он. И риски те же самые. Помещения, где проходят судебные заседания, - повышенной опасности. Всегда могут найтись люди, участники процесса, недовольные результатами, и нельзя заранее предугадать, как они себя поведут, во что выльется их раздражение и обида. Озлобление некоторых людей таково, что они способны разнести в клочья все здание суда. Наша задача по максимуму – предотвратить или вовремя остановить агрессию, действия, связанные с насилием, обеспечить безопасность персонала и посетителей».

Важно найти правильное соотношение оборудования СКУД и персонала. Контроль на внешнем периметре должен обеспечиваться достаточным числом охранников. Но все же главное – обеспечить координацию действий полиции и представителей частного охранного предприятия. В ожидании сложных, громких, скандальных судебных процессов все они встречаются и вместе обсуждают вопросы обеспечения безопасности до мельчайших подробностей. В том числе, рассматривается вопрос о связи с прессой, так как корреспондентам не всегда разрешается присутствовать в зале заседаний, и важно точно, выдержанно информировать прессу о происходящем в помещении суда.

Инструкция по защите паролей

Журнал Chief Security Officer (8 января 2016) опубликовал в качестве примера инструкцию, разработанную в одной крупной финансовой организации, насчитывающей более 5 000 служащих:

Меняйте пароли каждые 3 месяца

Не выписывайте пароли на листках

Не храните пароли в онлайне без шифрования

Не используйте одни и те же пароли для разных целей (электронная почта, персональные аккаунты, интернет банкинг, служебные документы и т.д.)

Никому не передавайте паролей, включая коллег

Не раскрывайте пароли в телефонных разговорах

Не раскрывайте паролей в переписке

Не раскрывайте паролей своим начальникам

Не упоминайте пароли в присутствии других людей

Не допускайте намеков при формировании паролей (к примеру, моя фамилия)

Не раскрывайте паролей при заполнении кадровых анкет или секретных документов

Не раскрывайте паролей родственникам

Не раскрывайте паролей коллегам по работе, находясь в совместном отпуске, на вечеринке

Если кто-то требует раскрыть пароль, сошлитесь на данную инструкцию и поставьте в известность СБ или ИТ отдел

Если возникает подозрение о компрометации пароля, немедленно доложите менеджеру по информзащите и срочно меняйте все пароли

СБ регулярно проверяет надежность паролей. Если во время одной из таких проверок

пароль раскроется, его надо немедленно менять.

Как клиенты реагируют на утечки информации

За спиной Брэндена Уильямса 20 летний опыт работы в сферах бизнеса, технологий, информационной защиты. Недавно он провел собственное расследование, стремясь понять, влияют ли утечки пользовательской и иной корпоративной информации на поведение клиентов, на их отношение к организации после инцидента безопасности. О результатах исследования он рассказал в интервью журналу CSO Magazine (26 января 2016).

На вопрос журналиста, что подтолкнуло его к расследованию, эксперт ответил: «В руки попали некоторые статистические данные, согласно которым клиенты избегают обращаться в компанию, где взломаны базы данных, где скомпрометированы кредитные и дебитные карты. Среди упоминаемых корпораций – Target, Home Depot, Sears… Между тем, они продолжают работать, свои магазины не закрывают, и, похоже, неплохо себя чувствуют».

Уильямс решил сам расспросить пользователей товаров и услуг, подвергшихся атакам компаний. Полученный результат оказался совсем не тот, о котором заявляют статистики.

Исследование позволило сделать вывод, что если ставшая жертвой хакеров компания находится в шаговой доступности от дома пользователя, если там предлагаются не дорогие товары длительного пользования, а нечто повседневное и дешевое, то клиенты предпочитают завести новую кредитку и продолжать делать закупки в привычном месте.

Один из важных вопросов заключается в том, как ведут себя клиенты малого бизнеса. Если у малого предприятия хватает средств залатать дыру, образовавшуюся в результате несанкционированного проникновения злоумышленников в базы данных, заплатить все полагающиеся по закону компенсации и штрафы, то почему бы ему не продолжать свой бизнес, удерживая клиентов?

Ученого удивило, что 13% опрошенных в ходе исследования заявили, что вовсе не в курсе проблем с безопасностью в компаниях, чьими продуктами/услугами они пользуются регулярно. При этом замечено, что старшие поколения осведомлены об инцидентах лучше, чем молодежь. Женщины больше и лучше знают о том, что произошло с компанией, куда они обращаются (Target, Michaels), мужчины соответственно – с магазинами, посещаемыми ими (Home Depot, Sears).

В большинстве случаев утечки информации и компрометации сходны со стихийными бедствиями. Инциденты вызывают сбои в бизнес процессах, тратятся некие суммы на восстановление, но затем все операции возвращаются в нормальное русло.

Как распределяются расходы? Это затраты на расследование инцидента, судебные издержки, штрафы, гонорары для привлеченных специалистов и консультантов по информационной защите, средства на латание технологических дыр в ИТ структуре

компании, включая при необходимости покупку нового железа и софта, а также некоторые суммы на возможные компенсации пострадавшим клиентам и партнерам (обычно такие вопросы решаются через суд).

Бизнесмены должны позаботиться о том, какие данные они используют в повседневной работе, в нормальных операциях. Подумать, какой криминал эти данные могут заинтересовать, как уменьшить риски кражи и утечек информации.

Как убедить финансового директора в необходимости инвестирования в службу безопасности компании

Должностные функции финансового директора включают изучение потенциальных финансовых рисков, с которыми может столкнуться организация. Финансовый директор – непременный участник процессов планирования, прежде всего, связанных с бюджетом.

Эти моменты предопределяют необходимость теснейшего сотрудничества руководителя СБ и финдиректора/главбуха. Задача первого – разъяснить коллеге, где и в чем риски, как они могут повлиять на бизнес процессы, производимую продукцию, отношение клиентов, публичную репутацию. Но этого недостаточно. Важно объяснить стоящие перед организацией задачи в сфере управления рисками. Поскольку в реальности невозможно предупредить все риски, на 100% обезопасить компанию, то следует совместно с финансовым директором определить приоритеты охраны предприятия, принимая во внимание потенциальный ущерб при реализации тех или иных угроз. Совместный анализ служит наилучшей формой убеждения финансовой службы в необходимости адекватного финансирования СБ.

Брайан Контон в онлайновом издании Chief Security Officer обращает внимание, что в целом руководящие лица в бизнес компаниях больше внимания стали уделять вопросам безопасности, прежде всего, из-за успешных хакерских взломов сетей крупнейших корпораций (Sony, Madison, Ashley и других), повлекших огромный финансовый и репутационный ущерб. В ряде громких случаев управляющие менеджеры были вынуждены увольняться. Это уроки не только для первых лиц, но и для финансовых менеджеров, которые осознают, что рискуют лишиться места, если расследование инцидентов безопасности укажет в числе причин на недостаточное финансирование охраны и безопасности предприятия.

Автор статьи рекомендует в работе с финансистами (в рамках одной организации) иметь в виду следующие моменты:

• Помогать финансовому директору в уяснении особенностей компании с точки зрения выпускаемых продуктов и/или услуг, ее клиентской базы, рыночных позиций. Это необходимо для понимания информационной составляющей бизнеса, без которой организация не может нормально существовать, осознания, что и почему следует защищать в первую очередь.

• Некоторые организации являются одновременно объектом внимания для разного

рода злоумышленников: хакеров-одиночек и любителей, организованной киберпреступности и кибер-шпионов... Другие компании могут привлекать к себе внимание одной из перечисленных категорий. Знание, откуда исходит угроза, что собой представляют потенциальные взломщики, какими способами действуют, совершенно необходимо для правильного выбора инструментов защиты. Опережающие меры безопасности, адекватные реальным рискам, обеспечивают минимизацию потерь в случае инцидента, быстрое восстановление нормального бизнес процесса.

• Так как финдиректор непосредственно работает с бюджетом организации, его роль в принятии решения об инвестировании в охрану предприятия, в информационную защиту недооценивать нельзя. Особенно это касается тех статей бюджета, которые предусматривают ежегодное тестирование систем безопасности (симуляция несанкционированных вторжений), курсы обучения и тренингов для охранников и служащих компании, проверки на реагирование с имитацией инцидента и тому подобное.

Банковский сектор: кибер-риски партнерства

Канадские банки давно и заслуженно пользуются отличной репутацией в мире финансов. Но в 2015 году выяснилось, что главная угроза их доброму имени исходит от разветвленных партнерских связей, которыми пытаются воспользоваться преступники. Об этом пишет вице-президент компании Bae Systems Applied Intelligence Дейл Гуз в онлайновом издании Canadian Security Magazine (October 08, 2015).

Традиционно банк со временем обрастает сотнями и тысячами связей с бизнес партнерами, не говоря уже об армии частных клиентов. В наше время взаимодействие со сторонними организациями и лицами в значительной и все возрастающей степени осуществляется с использованием интернет технологий. Именно этот момент представляет наибольшую угрозу.

Отчеты о хакерских атаках отчетливо показывают, что именно уязвимости в системах защиты партнеров, а не самих банков, становятся главной причиной компрометации банковских баз данных. Финансовые организации, как правило, обладают мощными защитными программными редутами, способными отразить самые изощренные прямые нападения хакеров. Но это не относится к их многочисленным внешним партнерам и тем инструментам, которыми последние пользуются: платежные терминалы и процессоры, центры хранения и обработки данных, юридические конторы, аудиторские компании, консультанты, поставщики офисного оборудования и тому подобное. Вся эта густая сеть взаимодействия и взаимозависимости сегодня действует на базе электронных коммуникаций, используя которые, преступники нащупывают подходы к банковским счетам и прочей важной информации.

Угроза реальна и на кону большие деньги, предупреждает канадский журнал. По данным доклада о расследованиях случаев преднамеренного взлома банковских баз

данных, подготовленного компанией Verizon, 75% всех атак на банки Канады первоначальной целью имели партнеров, а через них уже сами банки. Такая многоходовая операция занимает от одного часа до суток. Получается, что те огромные ресурсы, которые банки бросают на свою защиту от киберкриминала, сводятся практически к нулю слабостями и уязвимостями систем безопасности третьих сторон. Относительно легкая доступность последних для злоумышленников часто объясняется тем обстоятельством, что работающие там специалисты по интернет технологиям свои наилучшие качества проявляют при реагировании на инцидент, но мало внимания обращают на защиту хранилищ данных, на меры контроля за доступом в сети, особенно дистанционном, на работу с пользователями корпоративных сетей.

Автор публикации в канадском издании предлагает в отношениях с партнерами следовать таким рекомендациям относительно кибербезопасности:

• Тщательно выбирать бизнес партнеров и строить взаимоотношения с учетом потенциальных киберрисков

• Очерчивать строго определенные рамки обмена информацией через электронные коммуникации

• Определять, где в системе взаимодействия могут возникнуть потенциальные угрозы

• Принимать совместные меры для минимизации рисков путем использования метрик, проверок и тестирования, проведения аудитов

• Использовать полученные результаты тестирования для укрепления систем обороны от хакеров

Товарные потери увеличиваются

Сокращение инвестиций в охрану предприятия оборачивается ростом потерь. Это правило особенно верно в отношении розничного бизнеса, пишет Марк Таралло в журнале Security Magazine (февральский выпуск, 2016).

Общие товарные потери ритейлеров включают в себя мелкие магазинные кражи посетителями (шоплифтинг - shoplifting), злоупотребления со стороны персонала и партнеров, административные промахи. Такие потери в США возросли в 2015 году на 0.7% по сравнению с предыдущим годом. Такая же тенденция и в мировой статистике.

В чем причины? Корни вырастают из конкретной экономической ситуации. Хотя экономика США уверенно растет, 47.6 миллионов американцев сидят на продуктовых карточках, 51% населения зарабатывает в год менее 30 тысяч долларов, что по меркам этой страны совсем немного, едва хватает сводить концы с концами. Более того, в то время как прибыли бизнеса увеличиваются, рост зарплат существенно отстает.

Не удивительно, что многие ограничивают свои расходы минимально необходимыми тратами. Застой потребительского спроса вынуждает компании сворачивать торговлю. В США за последний год закрылись без малого 10 000 розничных предприятий. Другие

компании вынуждены сокращать расходную часть своего баланса, нередко включая строчку «предотвращение потерь» (loss prevention). Согласно одному из солидных исследований, две трети опрошенных ритейлеров планируют в 2016 году либо сократить, либо оставить на прежнем уровне эту строчку бюджета. Между тем экономия на копейку здесь чревата убытками на рубли.

Рост товарных потерь отчасти обусловлен нерешенной пока проблемой организованной преступности. Криминал любит шарить по магазинным полкам, так как похищенные вещи нетрудно сбыть через интернет. 97% торговых предприятий стали жертвами оргпреступности в этой сфере в 2015 году (для сравнения: в 2014 году таких было менее 88%).

Что касается мелких краж посетителями торговых точек, то в обществе они воспринимаются как мало рискованный промысел, тем более, если речь идет о крупной торговой сети. Внимание им уделяется недостаточное.

У бизнесменов болит голова в основном из-за краж, осуществляемых персоналом магазинов. В каждом втором торговом предприятии США этот вид воровства приносит наибольший ущерб. Главные причины распространения подобных преступлений – слабые бэкграундные проверки нанимаемого персонала, плохой контроль со стороны администрации, ставка на работников с неполным рабочим днем (особенно в пик зимних новогодних, рождественских продаж – тогда же отмечается и пик воровства).

На общем фоне скромных затрат на борьбу с воровством выделяется стремление ритейлеров тратить деньги, прежде всего, на видеонаблюдение (83% опрошенных), тревожную сигнализацию (78%), на увеличение числа охранников (63%).

На пути модернизации СКУД

Крупнейший оператор скачек в Канаде Woodbine Entertainment Group пришел к выводу, что использовавшаяся на протяжении лет система охраны не очень надежна и не спасает от злоумышленников и нарушителей установленного порядка прохождения в офисные помещения.

Пятнадцать лет тому назад перед двумя главными входами в офис были установлены турникеты с оптическим контролем и тревожной сигнализацией. Включение сигнала тревоги сопровождалось автоматическим блокированием прохода. До поры до времен система работала исправно. Но потом поставщик системы вышел из этого бизнеса, возникли проблемы с запчастями для стареющей физически и морально техники.

«Возникла необходимость в новой СКУД, недорогой и в то же время более эффективной» - говорит директор по вопросам охраны и безопасности Робин Субрамани. В организации использовались электронные пропуска, как на вход, так и на выход. Это давало свои преимущества для контроля над потоком людей. К примеру, всегда можно было быстро установить, сколько людей в здании в любой данный момент, что совсем не лишне, например, при пожаре.

Однако, с годами служащие компании научились ловчить при потере или оставлении пропуска дома. В частности, применяли распространенный везде прием прохода впритирку. Этот же прием служит и злоумышленникам.

Поначалу присматривались к новым аналогичным турникетам, но цена ряда предложений представлялась чересчур высокой. Наконец, остановили свой выбор на системе Door Detective CL, конфигурация которой не позволяла нарушителям пролезть незамеченным. Для проверки и испытания установили эту систему в одном из подъездов. Новая система оказалась менее громоздкой по сравнению с предшествовавшей. Ее адаптировали к принятому в организации порядку проверки пропусков и интегрировали с видеонаблюдением. Провели тренировку с персоналом.

Все пришли к заключению, что пользоваться ей удобнее. Служащий прилагает свой пропуск к считывателю. Если процесс аутентификации проходит успешно, дверь открывается. Он (она) входит, следом идут другие и тем же способом проверки проходят внутрь. При этом дверь остается открытой, если пользователи идут один за другим без перерыва. Система снабжена сигнальными лампами и звуковым сигналом тревоги. Звуковой сигнал усилили.

Любой вид тревоги немедленно привлекает внимание дежурного офицера охраны, имеющего возможность отследить инцидент по видеомонитору. Функция архивации позволяет проводить расследования. СКУД исключает возможность сговора или незаметного проскальзывания. Функции авторизации входа и выхода разделены. Администрация всегда может выяснить, сколько людей в здании.

Как в Woodbine Entertainment Group, так и в других компаниях популярность получили беспроводные дверные замки с использованием технологии ENGAGE. Здесь применяется программное решение авторизации, очень удобное для служащих и охранников и особенно пригодное для использования внутри зданий, например, для охраны компьютерных комнат или помещений, где хранятся наиболее ценные вещи. Решение позволяет точно отслеживать, кто конкретно и где находится в любой данный момент. При этом приложение выпускается и в мобильном виде.

(по материалам журнала Security Magazine, январский выпуск)

Как улучшить свое резюме

Резюме представляет собой по существу маркетинговый документ, отмечают постоянные авторы журнала Security Magazine Дж. Бреннан и Л. Маттис. Кадровик по резюме и вашей внешности формирует первое впечатление и решает, стоит ли продолжать с вами работу на предмет возможного найма на искомую должность.

Авторы публикации предлагают несколько советов, как лучше готовить резюме.

Краткость – ключ к успеху

Те, кто приходит из органов правопорядка, частной индустрии безопасности, зачастую сбиваются на многословие в составлении резюме, стремясь достичь максимальной точности и правдивости в описании занимаемых в прошлом позиций и выполняемых функций. С чисто профессиональной точки зрения это неплохо. Однако, резюме должно в течение уже 20 секунд произвести нужное впечатление на кадровика, и потому обязано быть очень коротким. Если в прошлом вы осуществляли ту или иную программу безопасности, просто упомяните об этом и идите дальше. Конечно, за исключением случаев, когда эта программа или функция настолько сложна и

необычна, что может быть не понята и требует разъяснений.

Ориентация на искомую работу (должность)

Вы можете изложить полученные навыки и опыт в сфере охраны предприятия на десяти страницах, но кадровику дела нет до ВСЕЙ информации. Его интересует в основном то, что имеет прямое отношение к вакантной должности. Поэтому при составлении резюме необходимо фокусировать внимание на аспектах, вытекающих из должностной инструкции или описания задач и функций в анонсе. Если же хотите подчеркнуть широкий диапазон знаний и практических навыков, приложите к резюме перечень стоявших задач и функций.

Внимание дизайну

Резюме должно быть не только кратким, содержательным, но и привлекательным по оформлению. Бумага, шрифт, расположение текста - все имеет значение, не в последнюю очередь, для демонстрации ваших способностей в сфере межличностного общения, умения презентовать информацию в лаконичной и доступной манере.

Внимание словам

Старайтесь избегать слов «я» и «ответственный за...», которые приближают ваше резюме к описанию должностных обязанностей. Ни в коем случае не используйте должностную инструкцию по прежнему месту работы для написания резюме.

Как можно больше контактной информации

Не забудьте включить адрес проживания, номера телефонов (домашнего и мобильного, рабочего), адрес электронной почты. Неплохо также поставить даты по каждой из упомянутых в резюме позиций.

Бумажный вариант все еще важен

Хотя сегодня распространены электронные резюме, отсылаемые по месту возможной работы, для встречи с кадровиками, для собеседования совершенно необходимо иметь при себе бумажную версию.

Пять наиболее распространенных ошибок реагирования на инцидент безопасности

На них указывает на сайте csoonline.com эксперт К. Зуркус.

1. Неподготовленность

В организациях, не подготовившихся заранее к хакерским атакам, любое несанкционированное вторжение вызывает панику, растерянность, неверное реагирование, что, в конечном счете, отражается на статье непредвиденных расходов. При правильной заблаговременной подготовке организациям не составляет труда

оперативно ответить на вопросы: «Какая информация утекла?», «Как хакерам удалось пробраться в корпоративные сети?», «Как долго злоумышленники хозяйничали в базах данных?», «Откуда они пришли?» и тому подобное. Чтобы безошибочно и быстро получать ответы на эти и другие вопросы, организация должна иметь квалифицированный штат специалистов по информзащите, продуманные процессы и соответствующие технологии. В противном случае компания уподобляется слепцу, уверовавшему, что ему ничто не грозит.

2. Неверное определение масштабов инцидента

Организация может найти одну пробоину в системе кибербезопасности, а может насчитать таких дыр двадцать. Без точного понимания масштабов атаки невозможен адекватный ответ. Часто получается, что при восстановлении системы вы занимаетесь совсем не той проблемой, которой надо в данный момент.

3. Запоздалое обращение к услугам юристов

Нередко бывают ситуации, когда привлечение юристов критически необходимо, причем, чем раньше, тем лучше. Именно юристам надо доверить контакты с внешней средой, чтобы минимально снизить урон от утечки важной коммерческой информации, особенно связанной с клиентской базой, а также избежать преждевременного обнародования самого факта инцидента. О нем можно рассказать, когда уже проведена аналитическая работа и все аспекты прояснены: что случилось, как случилось, каковы результаты.

4. Ложное представление, что «миссия выполнена»

Непозволительно делать окончательный вывод, что в результате инцидента пострадали такие-то базы данных, или заявлять, что все восстановлено, в то время как вы еще не смогли оценить весь масштаб инцидента, все его последствия. Это означает задвигать проблему на задний план. Лучше скажите себе и другим: «Мы все еще изучаем ситуацию. Вот что мы уже знаем к данному моменту». Скоротечные выводы, в конечном счете, могут обернуться умножением реальных потерь, в том числе финансовых.

5. Непонимание корневых причин инцидента и вектора атаки

Если вы не поняли, почему и как преступникам удалось взломать ваши хранилища данных, если во время не определили вид атаки, то ждите повторного нападения завтра. Если не отремонтировали и плотно не закрыли дверь, через которую преступники проникли в вашу организацию, они явятся вновь. Вопрос времени – завтра, через неделю, через месяц. Надо принимать во внимание страх ошибиться, особенно если компании не хватает опыта и квалификации бороться с киберпреступностью. В этом случае рекомендуется обратиться к внешним экспертам и консультантам.

Насколько эффективны планы действий в чрезвычайной ситуации,

принятые в американских университетах?

Консалтинговая компания Margolis Healy, работающая с американскими университетами в сфере безопасности, провела в прошлом году опрос, давший следующие результаты.

86% респондентов, представителей разных вузов, показали, что в их организациях имеются планы действий в чрезвычайных ситуациях, ориентированные на риски и угрозы, характерные для данных заведений.

Однако, только 54.7% заявили, что в университетах проводятся занятия по реализации мер, предусмотренных планом действий, что совершенно необходимо для обеспечения эффективности такого плана при всех возможных угрозах.

В более чем четверти университетов вообще не проводятся учения на случай применения нападающим (нападающими) огнестрельного оружия – как «настольные» симуляционные игры, так и максимально приближенные к реальной ситуации тренинги.

31% респондентов отметили, что в их вузах нет персонала, который бы разрабатывал и в случае необходимости реализовывал бы оперативные планы. В колледжах двухгодичного обучения процент таких организаций достигает 41.2%.

Менее половины участников отметили, что в их организациях проводятся разборы по следам инцидентов безопасности, сверяются планы и инструкции, вносятся соответствующие директивы.

Более 60% не верят, что их организации располагают персоналом достаточно высокой квалификации для обеспечения надлежащей безопасности (речь идет как о собственных охранниках, так и работающих по аутсорсингу).

Взгляды на безопасность у различных категорий лиц (проректор, руководитель СБ, лидеры студенческих организаций) существенно разнятся. Например, когда дело касается социальных медиа, то, как показало исследование, 64% вузов проводят мониторинг социальных сетей в открытом доступе, которые так или иначе связаны с их организацией.

Но при этом 75.6% университетских руководителей уверены, что такой мониторинг проводится, а среди администрации кампусов в этом уверены менее половины опрошенных.

Рецензия

A Law Enforcement and Security Officers’ Guide to Responding to Bomb Threats
Jim Smith; Reviewed by Hugh J. Martin

Это третье издание книги, посвященной вопросам противодействия террористическим

угрозам, конкретно – бомбистам. Основной фокус внимания автора – первые действия при возникновении опасности взрыва. Подробно рассматриваются виды взрывных устройств, используемых террористами.

Автор книги Джим Смит имеет за спиной 30-летний опыт работы в сфере безопасности и охраны здоровья. Тщательно проанализированы все процедуры и меры, позволяющие сохранить жизнь при угрозе взрыва бомбы. Перечислены и объяснены всевозможные ситуации, при которых совершаются террористические акты.

Тест написан доходчивым, понятным языком и должен занять достойное место в индивидуальных и ведомственных библиотеках, как правоохранительных организаций, так и частных охранных предприятий.