Охрана предприятия

№3 (31), 2013

Оглавление

Охрана предприятия за рубежом

На охрану американских школ заступают вооруженные охранники

Канадский Форум профессионалов и партнеров в сфере корпоративной безопасности

Книжное обозрение

Basic Private Investigation: A Guide to Business Organization, Management, and Basic Investigative Skills for the Private Investigator.

Наиболее востребованные компетенции руководителя СБ в 2013 году

Под таким названием онлайновый журнал Chief Security Officer (06 March, 2013) опубликовал опрос ряда руководителей охранных предприятий и служб США.

В преамбуле публикации утверждается, что набор качеств и умений, необходимых для успешной карьеры специалиста в сфере охраны и безопасности, каждые несколько лет претерпевает определенные изменения. Респондентов спрашивали, какие, по их мнению, компетенции сегодня наиболее востребованы. Вот некоторые, наиболее показательные ответы:

Способность определять зарождающиеся тенденции, актуальные потребности бизнеса. Это позволяет руководителю СБ решать, какие специалисты, с каким опытом и конкретными знаниями ему нужны сегодня и в ближайшие годы.

Хорошее знание новейших технологий физической охраны и информационной защиты. Особенно важно умение разбираться в программных продуктах цифрового видеонаблюдения и видео аналитики. Используемые в настоящее время технологии обрушивают на охранников массу информации, в которой легко затонуть. Работа с информацией требует специальных знаний и умений. Поэтому профессионалам охранного дела необходимо овладевать знаниями интернет технологий и/или привлекать соответствующих специалистов со стороны.

Продвинутое знание технологий защиты информации. В наше время уже недостаточно уделять исключительное внимание охране физического периметра организации. Не по дням, а по часам умножается спрос на экспертов в области защиты информации, особенно разбирающихся в таких вопросах как многоуровневые модели защиты, технологии классификации данных, биометрика. Неудивительно, что и в университетах, и в индустрии безопасности растет число курсов и учебных программ по этим направлениям.

Деловая хватка и финансовая сообразительность. Руководитель СБ обязан понимать,

как работа его подразделения реально влияет на итоговую строчку корпоративного баланса. Это важно с разных точек зрения, в том числе для понимания и контроля потенциально уязвимых аспектов деятельности компании, таких, например, как аутсорсинг, хранение финансовых и иных корпоративных данных, лакомых для киберпреступников. Поэтому растет спрос на профессионалов охранного дела, разбирающихся в вопросах бизнеса. В крупных корпорациях от руководителей СБ требуют дипломы МБА и/или практический опыт предпринимательской работы.

Отличные способности общения. Надо уметь не только доходчиво разъяснять менеджменту проблемы охраны и безопасности, но и убедительно демонстрировать их значение для итоговых результатов компании.

Приспособляемость к рыночным и технологическим изменениям. Здесь важно стремление постоянно учиться, пополнять запас знаний и навыков. Насколько быстро меняется рыночная среда, настолько же умело и гибко нужно учиться выявлять и решать новые проблемы.

Технологии виртуального обучения и тренинга

Шелби Берд, Партнер компании Iomnis Surveillance Solution, в статье онлайнового издания securitymagazine.com (1 декабря 2012 года) рассказывает о современных технологиях, которые все чаще используются в тренинговых программах охранников. Их особенность заключается в создании виртуальных проблемных ситуаций и виртуальном же их разрешении.

Технологии виртуального тренинга позволяют моделировать самые сложные обстоятельства и ситуации, ставить перед слушателями трудные задачи, воссоздавать опасные, рискованные ситуации. Полное погружение в сценарные игры стирает видимость границы между реальностью и виртуальным миром, создает условия для поведенческого анализа, а также детального тестирования политики и процедур, принятых в компании.

Одно из важнейших преимуществ виртуального тренинга перед обычными учебными программами – экономическая эффективность. Охранники проходят курс повышения квалификации «без отрыва от производства», непосредственно в компании.

Сегодня мировые рынки предлагают разные технологии виртуального обучения. Наиболее распространены 3D шлемы HDM (head mounted display, шлем-дисплей – специальное устройство, используемое в системах виртуальной реальности), LCD/ LED (жидкокристаллические индикаторы, светодиоды), беспроводные опции…

Выбор правильного девайса исключительно важен, так как с его помощью осуществляется интерактивная связь между пользователем и виртуальным миром, создаются виртуальные условия, в которых действует и принимает решение слушатель курсов обучения.

Наиболее совершенные технологии обеспечивают полное подобие реальности. Самое впечатлительное измерение – скорость, с которой моделируются ситуации. Экономия

на времени, которое требуется для программирования и моделирования сценария, позволяет добиваться высоких тренировочных результатов в сжатые сроки, что непосредственно влияет на конечную стоимость всей учебной программы.

Сегодняшние технологии были немыслимы еще несколько лет назад. Виртуальная реальность возникает из моделирования, из чертежа, из рисунка. Новации в этой сфере могут решать разного уровня задачи, с различными типами аналитических данных. Простые задачи заключатся в проверке и совершенствовании таких показателей как точность и время принятия слушателем правильного решения, последовательность действий, их результат. Более сложный уровень тренинга включает в себя контроль кровяного давления, частоты сердечного биения, а также проверку реакции слушателя на внезапные вспышки света, оглушающие звуки, необычные запахи, перепады температуры и давления и так далее.

Современные тенденции в видео аналитике

Билл Залуд опубликовал в онлайновом журнале Security Magazine (February, 2013) пространную статью о новейших аналитических технологиях в системах видеонаблюдения.

Одна из последних новинок – программное решение, позволяющее сжимать (суммировать) все движения за данный период времени в более краткий конспект: 24 часа в 15-минутный синопсис, что на 50% короче распространенных до недавнего времени продуктов.

Совершенствуется и видео аналитика, фиксирующая и реагирующая на анормальные движения и картинки. Оператор устанавливает стандарты и критерии объекта в поле зрения камеры. Появление анормальностей, отличающихся от стандартной картинки, автоматически фиксируется и либо идет одномоментно сигнал на пульт, либо отклонение от критерия отмечается специальным знаком для отложенного просмотра. Такая технология удобна для использования в торговых центрах, или, например, для фиксации переезда машиной железнодорожного полотна, где нет регулирующих шлагбаумов. Также может использоваться для наблюдения за движением транспорта и пешеходов на улицах и площадях. Камеры, оснащенные продвинутыми процессинговыми технологиями, конечно, стоят относительно дорого, но цены из года в год снижаются.

Стали появляться аналитические технологии, адаптированные для специальных крупных мероприятий. Таким большим событием, в частности, будут Зимние Олимпийские игры в Сочи. Компания Nice Systems по заказу российской стороны выпустила предназначенную специально для Сочи систему видео мониторинга улиц и городских, в том числе спортивных, объектов. Говорит Сергей Черепов, директор ситуационного мониторинга Игр в Сочи: «В ближайшие годы ожидается быстрый рост населения и экономики Сочи, что ставит новые, более сложные задачи обеспечения безопасности и обуславливает повышенные требования к контролю за повседневной жизнью города» (там же).

Другое направление развития видео аналитики – фиксация особенностей

человеческого поведения, таких как беспокойство, смятение, возбуждение, агрессия….Это технология ассоциативного анализа данных предполагает фиксацию и сопоставление каждого движения, изменения объекта (человека) с запрограммированным набором стандартов поведения (жестов, походки и т.п.). Процесс отслеживания агрессивности/возбужденного состояния проходит в режиме реального времени. Одновременно ведется подсчет людского трафика в минуту, в час, в сутки. Такие системы могут быть использованы в торговых центрах, в аэропортах, музеях и других общественных местах. Конечно, такие «умные» камеры с аналитикой стоят выше средних рыночных цен.

Один из путей совершенствования – минимизация ложных сигналов. Видео аналитика способна различать существенные и несущественные изменения. В числе последних – листопад, воздействие ветра на растения, появление животных, т.е. изменения, не несущие реальной опасности или угрозы. Технология распознавания отфильтровывает происходящие изменения и принимает решение, отправлять тревожный сигнал или нет. Такие системы более всего подходят для мониторинга ситуации в портах, вокруг удаленных объектов коммунальных служб, подверженных воздействию экстремальных (например, погодных) условий.

Конкурс на безопасный пароль

Группа специалистов по шифрованию из Национального института стандартов и технологий США (National Institute of Standards and Technology) объявила открытый конкурс на новый хэш алгоритм для паролей на веб-сайтах с целью затруднить хакерам задачи взлома онлайновых баз данных (хэш-кодирование или хэширование означает способ обеспечения ключевого доступа к элементам данных; каждый элемент данных хранится с соответствующим ключом, который обрабатывается при помощи хэш-функции; в настоящее время практически ни одно приложение криптографии не обходится без использования хэширования).

Организаторы конкурса открыли специальный сайт, куда можно направлять свои идеи https://password-hashing.net/index.html. Сайт доступен до 31 января 2014 года. Здесь можно ознакомиться с техническим руководством, разъяснениями, по каким критериям оценивается каждый проект. Призов и премий не предусмотрено.

Национальный институт стандартов и технологий – головная в США организация по утверждению и контролю за стандартами шифрования и хэш алгоритмов. Последние предназначены для разбивки простых текстовых паролей на группы букв и цифр, что создает трудности для хакерских попыток проникнуть в онлайновые базы данных. В числе наиболее распространенных сегодня алгоритмов – SHA (Secure Hash Algorithm), разработанный правительственной организацией U.S. National Security Agency. Этот алгоритмический стандарт имеет различное практическое применение, но малопригоден для шифровки паролей на веб-сайтах. Вопрос скорости и времени. Чем быстрее хэшируется (а, следовательно, и дешифруется) пароль, тем легче хакеру овладеть им. И наоборот, чем протяженнее во времени процесс дешифровки, тем сложнее его разгадать.

Поэтому организаторы конкурса, формулируя свои задачи, упирают на то, что новый стандарт паролей должен замедлить процесс входа в веб-сайт (онлайновые базы

данных), но не настолько, чтобы пользователь нервничал от слишком долгого ожидания. В этом заключается определенное противоречие, замечает один из членов жюри конкурса, специалист из Швейцарии Жан-Филипп Омассон: «С точки зрения безопасности, чем медленнее процесс, тем лучше. С точки зрения пользователей, чем быстрее, тем лучше. Необходимо найти правильный баланс между этими противоположными условиями» (Chief Security Officer, February 15, 2013).

Хотя хэш алгоритм SHA известен и используется уже многие годы, хэширование паролей на веб-сайтах и мобильных дивайсах – нечто новое, и здесь для ученых и специалистов в области шифрования – целина открытий.

Отставание технологий шифрования позволяет хакерам проводить успешные атаки. Так, например, им удалось в прошлом году взломать защиту социальной сети LinkedIn, и миллионы хэшированных паролей были украдены, расшифрованы и размещены на русском форуме хакеров.

Надеясь на появление продвинутых технологий шифрования паролей на веб-сайтах и мобильных носителях информации, организаторы конкурса, однако, не рассчитывают, что это быстро скажется на широком внедрении новых стандартов. Омассон полагает, что не раньше чем через 10 лет результаты конкурса и иные предпринимаемые усилия в этом направления приведут к широкому осознанию необходимости принять на вооружение и использовать более безопасные пароли.

(по материалам онлайнового издания Chief Security Officer)

Что такое социальная инженерия и как от нее защищаться

Часть 2 (начало см. журнал №30)

Социальные сети открыли новые возможности для мошенников. Преступники крадут пароли, проникают в аккаунты, а затем представляются вам в Фейсбуке от имени других людей, в том числе реальных друзей.

Один из распространенных приемов - сигнал SOS: злоумышленник под именем «друга» пишет, что его ограбили во время путешествия (обычно в другой стране) и просит выручить деньгами до возвращения домой. Редактор журнала «Охрана предприятия» однажды попал в аналогичную ситуацию, когда на его электронный адрес пришло сообщение от имени (и с адреса!) хорошо и давно знакомой американки, которая будто бы «подверглась нападению, избиению, находясь в Лондоне, и лишилась всех документов и денег». Естественно, предлагалось проявить сочувствие и переслать взаимообразно, «до возвращения домой», тысячу-другую долларов на указанный в письме лондонский счет. Первая реакция – помочь, но когда на уточняющий вопрос редактор получил странный ответ, зародились первые подозрения, и элементарная проверка (звонок в Нью-Йорк на домашний телефон) сняла последние сомнения в том, что действуют аферисты…

«Если вам удалось получить доступ в личный аккаунт пользователя социальных сетей, то не составляет труда узнать многое о его семье и работе, - говорит Грэхем Клалей,

старший консультант охранной компании Sophos, - например, кто его/ее супруг, когда и где последний раз отдыхали,…Получив информацию, не сложно выдавать себя за другого» (Chief Security Officer, December 20, 2012).

Другой прием, нередко используемый преступниками в социальных сетях, - намеренная дезориентация в поиске товаров и услуг через фальшивые линки и ложные «коммерческие» сайты. Особенно популярна эта схема в предпраздничные дни. Специально к Рождеству и Пасхе в сетях появляются «благотворительные фонды».

Но есть и реальные сайты, помогающие бороться с социальной инженерией. Брайан Брашвуд создал сайт под именем «Scam School» («Школа аферистов»). Он выделяет четыре базовых приема, с помощью которых жулики обдуривают людей.

1. Внушают доверие. Они не подкрадываются сзади, а, напротив, подходят « с открытой душой», делают все, чтобы обратить на себя внимание.

2. Дают или что-то делают для вас. Даже ничтожная услуга внушает доверие и симпатию.

3. Используют юмор. Он способен обезоруживать, снимать подозрения.

4. Высказывают внешне разумные предложения. Люди обычно охотно отвечают на идеи, запросы, которые им кажутся адекватными, интересными.

В социальных сетях мошенники делают упор на использование таких наклонностей как страх и любопытство. Например, посылают вопрос: «вы себя еще не видели в видео ролике?» с приложением «плохой» ссылки.

У специалистов по фишингу популярна такая наживка: «ваш банковский счет скомпроментирован, немедленно кликните на этот линк и войдите в систему для восстановления счета».

Иногда, прикрываясь трендами известных интернет магазинов, жулики присылают уведомления типа: «вы не оплатили покупку, нажмите здесь для оплаты».

Чтобы избежать обмана, эксперты советуют людям «быть мелочно-дотошными, и даже чуть-чуть параноидально недоверчивыми, поскольку вы всегда до конца не понимаете, что от вас в действительности хотят» (там же).

Как показывает опыт, жертвами мошенников становятся и менеджеры, и руководители компаний. Например, преступники умело используют в своих аферах пристрастие людей к последним технологическим новинкам и их боязнь продемонстрировать перед всеми собственную наивность и глупость.

Разведка как компонент корпоративной безопасности

На вопрос о том, какие основные тенденции сегодня прослеживаются в работе

руководящих сотрудников корпоративных служб безопасности, Джерри Бреннан, главный оперативный офицер (chief operating officer) в СБ компании Security Management Resources, не задумываясь отвечает: «интеграция и растущие требования к качественной и своевременной разведке как составной части процесса бизнес решений, принимаемых на всех уровнях» (securitymagazine.com, December 2012).

Конечно, отмечает Бреннан, и раньше элементы разведки в разной степени присутствовали в деятельности компаний. Но сегодня значение разведки, работающей на упреждение, возрастает многократно. Посмотрим на то, что собой представляет модель управления рисками с точки зрения принимающих решения менеджеров. С позиции совета директоров идеальная модель должна просчитывать потенциальный ущерб для компании от возможных событий и инцидентов, подсказывать, какие риски оправданы, а какие нет. А для этого требуется анализировать все ключевые функции, текущие проекты и процессы в компании, пытаться понять, где и какие имеются уязвимости, чего не хватает для снижения уровня рисков.

И в этом контексте особое значение приобретает упреждающая разведка, призванная собирать и анализировать точную и надежную информацию, помогающая принимать верные, «зрячие» бизнес решения. Потребителями продукции разведки являются как топ менеджеры, так и управленцы среднего звена.

Бреннан перечисляет сферы приложения разведки, наиболее популярные в настоящее время в системе управления рисками.

Геополитические риски. Выявление международных конфликтных зон, угрожающих финансовой и оперативной стабильности организации, помощь в определении рамок сдерживания таких угроз, минимизации рисков и сохранения бизнеса.

Кибер угрозы. Здесь важно своевременно просчитать, какие хакерские атаки и с какой целью могут произойти.

Аудит. Финансовая и юридическая экспертиза. Поддержка в вопросах слияния и присоединений, создания совместных предприятий, сотрудничества с поставщиками и партнерами.

Конкурентная разведка. Сбор, анализ информации о конкурентах, сквозной обмен информацией между всеми подразделениями компании.

Контрразведка. Выявление собственных слабостей, уязвимостей, помощь в их устранении.

Современная модель управления рисками предполагает сочетание таких компетенций как умение планировать, аналитические данные, креативные разведывательные способности, заключает Бреннан.

Как создать эффективную команду для анализа угроз

Этому вопросу посвящена статья Тони Миллера в журнале Security Magazine, February

2013. Тони Миллер, менеджер BT Global Services, обладает 20-летним опытом работы в сфере информационной безопасности, руководил одно время группой специалистов по выявлению уязвимостей в системах безопасности финансово-кредитных организаций.

Миллер пишет, что постоянный мониторинг и тестирование систем безопасности на предмет выявления потенциальных угроз необходимы каждому бизнесу. Главная здесь задача – держать менеджмент компании в курсе существующих и потенциальных угроз, разъяснять, как эти угрозы могут влиять на деятельность организации. Проверка надежности систем защиты и безопасности призвана не только обнаруживать слабости, но и находить взаимосвязь между уязвимостями и реальными угрозами. Создание группы по анализу угроз требует методического подхода и тщательного планирования.

Начинать надо с плана. Сформулировать стоящие задачи. Определить, на какой уровень менеджмента рассчитан итоговый отчет, какого характера рекомендации там могут быть. Решить, будет ли создаваемая команда отслеживать осуществление рекомендаций, или этим займется другая структура в организации.

Когда задачи, обязанности и функции внутри команды определены, все внимание – кадровому заполнению. Тони Миллер твердо уверен, что группу следует комплектовать специалистами, имеющими а) практический опыт работы в сфере корпоративной безопасности, желательно в сегменте информационной защиты; б) знание профильного бизнеса компании; в) организационные способности, прежде всего, навыки делового общения с топ-менеджментом. В идеале в команде должны быть представлены самые разные специалисты – программисты, системные интеграторы, офицеры по безопасности, эксперты по вопросам хакерских проникновений, бизнес аналитики.

Следующий шаг – разработка методологии. Процесс тестирования может охватывать самые разные аспекты и вопросы. Их надо определить. Равно как и обозначить информационные ресурсы – публикации, блоги, онлайновые специализированные издания, новостные ленты, ... Не менее важно иметь полную картину развития бизнеса компании, учитывать происходящие изменения в бизнес процессах, структуре и т.д.

Совершенно необходимо решить, кому и как команда будет докладывать о возникающих угрозах:

- информация на регулярной основе или по времени возникновения новых угроз;

- формат отчетов;

- классификация угроз по степени опасности;

- способы немедленного информирования при выявлении угроз повышенной опасности;

- список лиц, кому будут направляться регулярные отчеты и срочные сообщения, требующие немедленного реагирования.

И последнее – разработка стандартов и политик, способствующих успешной реализации избранной методологии.

Как проводить внутренние расследования

Этой теме посвящена статья в онлайновом журнале Security Magazine (февральский выпуск 2013 года).

Джеймс Рэтли, обладающий 30-летним опытом внутрикорпоративных расследований утверждает: «Все просто, если у вас на руках есть конкретный план».

Другой эксперт, Джо Форд, выделяет в процессе расследования четыре последовательных этапа:

1. Начальный этап – сбор информации об инциденте, когда и как произошел.

2. Анализ. Каковы возможные последствия, исходя из собранных документов.

3. Опросы служащих с целью понять, кто жертва, а кто виновник.

4. Обращение в полицию. Привести в порядок собранную информацию, все имеющиеся на руках документы и передать в полицию для дальнейшего расследования, но только при условии, если вам понятно, что произошло и каковы последствия.

Часто повторяемая ошибка – нарушение последовательности. Например, когда начинают опрашивать сотрудников еще до того, как собраны все документы. Документы надо предварительно проработать, чтобы четко понимать, какие вопросы и кому следует задавать – свидетелям, жертвам, подозреваемым.

Что касается свидетелей, то необходимо строить вопросы кратко, понятно, безотносительно от того, что утверждает подозреваемый.

Допрос подозреваемой личности – более сложная процедура. Для проведения допроса Джеймс Рэтли приезжает рано утром, еще до того, когда служащие приходят на работу. Заранее выделяется помещение. Это не должна быть рабочая комната. Мобильники отключаются, чтобы не отвлекать внимание. Рэтли использует такой прием: он выходит из комнаты под предлогом заказать чашку кофе или позвонить, но перед этим говорит собеседнику, что у него есть нечто очень важное сообщить. Беспокойство и страх помогают: подозреваемый хочет выяснить как можно скорее, что именно знает расследователь, он нервничает. По возвращении Рэтли обычно минут пятнадцать говорит о вещах отвлеченных, заставляя собеседника еще более нервничать. Наконец, произнеся общую фразу «мне известно, что произошло», расследователь переходит к прямым вопросам по существу. Вопросы задаются в манере, скрывающей от подозреваемого то, что расследователь не знает. Пусть подозреваемый говорит все, что хочет. Попытка оправдаться парируется документом, но документ предъявляется только тогда, когда подозреваемый отпирается. После того, как все пути к отступлению отрезаны, подозреваемый начинает рассказывать, как все было на самом деле. Весь допрос обычно занимает около 3 часов.

Хотя во многих случаях последующее вмешательство полиции неизбежно, эксперты предупреждают о нежелательности ее привлекать уже на ранних этапах внутрикорпоративного расследования. Вопрос: почему не поручить весь ход

расследования компетентным органам? Ответ экспертов: бюджет, деньги. Если ущерб оценивается в сумму менее 50 000 долларов, американские банки предпочитают не связываться с полицией. Во-первых, у полиции не всегда имеется опыт расследования преступлений, совершаемых «белыми воротничками». Во-вторых, у каждого полицейского следователя на столе куча других дел. В-третьих, полицейский не знает специфики компании, ее бизнеса так, как это знают сотрудники собственной СБ.

Как проводить расследования в зарубежных филиалах и представительствах глобальных корпораций

Острая международная экономическая конкуренция заставляет многие компании выводить свой бизнес в районы мира, где есть сырьевые ресурсы и более дешевая рабочая сила. Но там они зачастую сталкиваются с такими проблемами как политическая нестабильность, высокий уровень коррупции и преступности. Шоун Кларк рассуждает на эту тему в публикации журнала Security Magazine (February, 2013).

Существуют две базовые структурные модели службы безопасности в транснациональных компаниях: централизованная и децентрализованная. Централизованная модель, предполагающая концентрацию штата сотрудников в основном офисе компании, в штаб-квартире, обладает преимуществами с точки зрения учебной подготовки, коммуникации, взаимодействия, создания дружной командной атмосферы, выстраивания отношений на основе доверия. Но эта модель хороша, когда риски минимальны, ситуация в регионах бизнеса спокойная, особых проблем для СБ не рождает.

Но так бывает редко. В большинстве случаев картина обратная, далекая от идиллии. И тогда наиболее эффективной себя показывает структура децентрализованная, с людьми и техническими ресурсами непосредственно в районах производства, ведения бизнеса. Для такой модели предпочтительно, чтобы в штате СБ работали представители коренного населения, владеющие языком страны, хорошо знающие местную культуру, традиции и обычаи, понимающие, каким образом гендерные, религиозные и прочие цивилизационные особенности могут влиять на бизнес.

Иметь местные кадры в структуре СБ также важно с точки зрения кооперации с региональной полицией, другими государственными и общественными институтами, без тесных контактов с которыми невозможно отслеживать и прогнозировать развитие ситуации, собирать и анализировать материал об инцидентах, происходящих с другими международными корпорациями, работающими в том же регионе. Для успешной работы необходимо знать, кто есть кто в данном городе или районе, кто имеет связи в судах, в местном правительстве, правоохранительных органах.

Время от времени возникает необходимость расследования фактов мошенничества и воровства, внутренних конфликтов и инцидентов в зарубежных филиалах и

отделениях корпорации. Автор статьи советует в таких случаях начинать с изучения местных законов о труде, заключенных контрактов и сделок, в первую очередь деталей, которые не укладываются в действующие (в корпорации) правила и нормы. Дело в том, что во многих странах, подчеркивает Кларк, местные власти не стремятся поддерживать иностранные компании в судах, а суды, как правило, берут сторону своих.

Международные конвенции и соглашения довольно сложны для понимания. Их надо как следует проштудировать, прежде чем начинать расследование. Но надо знать и местные законы. В некоторых странах, например, власти требуют информировать их о лицах, являющихся объектом расследования. Иногда местное законодательство предусматривает проведение расследования в жесткие сроки (до 30 дней). Незнание международного и местного законодательства применительно к теме расследования может обойтись очень дорого.

В ходе расследования выходцы из местного населения, работающие в структуре корпоративной безопасности, опять же незаменимы. Они знают язык, диалекты, что часто имеет решающее значение для успешной работы с подозреваемыми и свидетелями.

Как успешно пройти процедуру найма в охранное предприятие

В онлайновом издании Chief Security Officer 4 февраля этого года опубликованы рекомендации для соискателя на работу в охранном предприятии:

1. Напишите и пошлите хорошее резюме, которое побудит работодателей пригласить вас для беседы.
2. Если вы из того же города (района), где расположен офис компании, то вам могут позвонить с целью уточнить те или иные моменты из вашего резюме. Поэтому желательно заранее приготовить факты, продумать примеры, подтверждающие резюме.
3. Заранее разузнайте, какой принят дресс-код в компании, чтобы одеться для встречи и беседы соответствующим образом.
4. В ходе собеседования не навязывайте свои темы, а просто внимательно слушайте, что вам говорят, что спрашивают, и четко отвечайте строго на вопросы. Ничего лишнего.
5. Работодатели обычно стремятся проверить соответствие резюме вашим реальным способностям и возможностям. Поэтому не оставляйте в резюме положения и характеристики, которые не можете подтвердить фактами.
6. Важно подчеркнуть свои сильные стороны. Но не забывайте и не скрывайте недостатки. Готовьтесь говорить о них, если зайдет речь.
7. Делайте упор на свое желание и способность внести полезный вклад в общее дело компании. Заранее приготовьте примеры из своего предыдущего опыта: как обнаружили угрозы, что сделали для их минимизации, для того, чтобы бизнес был лучше защищен и т.п.
8. Предварительно изучите компании, куда собираетесь посылать резюме, особенно на предмет их внутренней корпоративной культуры, которая, быть может, вам не

подходит.
9. Для предварительного исследования используйте онлайновые базы данных, включая такие ресурсы как LinkedIn, чтобы узнать как можно больше о тех, кто, возможно, будет с вами беседовать, оценивать, принимать решения. Не исключено, что в данной компании обнаружите знакомых, которые насытят вас полезной информацией перед собеседованием.
10. Проведя изучение и собрав определенную информацию, продемонстрируйте свое знание компании, заранее подготовив вопросы. Одни вопросы могут касаться используемых в компании охранных технологий. Другие – бизнеса компании.
11. Приготовьте вопросы, касающиеся делового стиля, принятого в компании, прежде всего потенциального начальника, коллег, с которыми предстоит каждый день общаться.
12. Демонстрируйте интерес к той позиции, на которую претендуете, но ни в коем случае не пережимайте, пытаясь выяснить, какое впечатление вы произвели.
13. Держитесь расковано, но не перестарайтесь: нельзя вести себя так, будто вопрос о приеме на работу уже положительно решен.
14. Кстати, не вздумайте опаздывать на встречу. Напротив, приезжайте за некоторое время до начала, чтобы успокоиться, привести мысли в порядок, морально подготовиться.
15. Заранее подумайте о дальнейших шагах после интервью. К примеру, если хотите контактировать по e-mail, попросите визитную карточку с контактами.

Эти рекомендации подготовил и опубликовал Джефф Снайдер, президент компании SecurityRecruiter.com, которая занимается рекрутингом в сфере корпоративной безопасности.

Больше тренировок – выше эффективность

Статья с таким названием на сайте securitymagazine.com от 1 декабря прошлого года рассказывает, как тренируют сотрудников в охранных структурах крупных частных организаций.

Даррелл Клифтон возглавляет службу безопасности в корпорации Circus Circus Reno, владеющей большим курортным отелем и казино в штате Невада. В его команде 54 штатных охранника. Каждый вновь приходящий не просто знакомится с местом работы, но в обязательном порядке начинает службу с академического курса обучения, 70 учебных часов. Затем – три недели «полевой практики» под присмотром опытного коллеги.

Для всего охранного персонала практикуются т.н. «освежающие» тренинги. Так, в частности, регулярно один или несколько охранников приглашаются на 10-минутный брифинг, во время которого проверяется их реакция, готовность принимать быстрые и правильные решения в самых разных, подчас неожиданных ситуациях, например, в случае ограбления в лифте отеля.

При этом особое внимание уделяется внешнему виду и манерам сотрудников СБ. Это и понятно. На курорте, куда люди приезжают отдыхать и развлекаться, охранники не

должны выглядеть тюремными надзирателями.

Клифтону удалось убедить владельцев корпорации в необходимости тренировок для обслуживающего персонала. Охранников хватает для поддержания порядка и безопасности в обычных, спокойных условиях. Но в экстремальной ситуации обязательно потребуется помощь всех, кто работает в отеле и казино. Скажем, во время угрозы пожара они должны помогать в эвакуации клиентов, в то время как служба СБ будет выполнять свои прямые обязанности. Кроме того, горничные, технические работники отлично знают расположение и состояние помещений, а, следовательно, обязаны обращать внимание на забытые в комнатах вещи, на оставленные опасные материалы, немедленно ставить в известность охранников.

Конечно, программы тренинга требуют прямых и косвенных затрат. К тому же письменные инструкции и материалы для тренингов приходится печатать для обслуживающего персонала на разных языках.

В нью-йоркском небоскребе Херста расположены редакции крупных изданий. Ими владеет династия газетно-журнальных магнатов, и атмосфера в корпорации поддерживается почти семейная. Хотя охранники в высотке нанимаются через охранное предприятие AlliedBarton Security Services, к ним относятся как к равноправным членам единого коллектива, одной большой семьи. Благожелательная среда позволила свести к минимуму кадровую текучесть.

В AlliedBarton Security Services все охранники проходят пятиступенчатую программу подготовки. Хотя 90% охранников приходят в корпорацию Херста, имея за плечами полный курс обучения, для всех работников СБ разработана специальный тренировочный курс, который ориентирован на самые разные функции – от оказания первой медицинской помощи до действий в самых сложных, экстремальных условиях, например, во время ураганов. Кроме встречи обычных, повседневных посетителей охранников обучают правилам приема вип-гостей, которые здесь не редкость. Программа тренинга также предусматривает дополнительные занятия по противопожарной и медицинской дисциплинам.

5 мифов вокруг работы с персоналом компании по вопросам защиты корпоративной информации

Ланс Спицнер, директор учебных программ консалтинговой компании SANS Securing the Human, размышляет на тему различных мифов относительно проведения тренингов для персонала организаций по вопросам защиты информации.

«Тренинг ничего не дает». Это в тех случаях, а их большинство, когда упор делается на простое соблюдение принятых в компании правил безопасности, а не на изменение поведения людей. Все ограничивается минимумом усилий – раз в год общее собрание по этим вопросам, может быть, еще выпуск квартальных внутренних бюллетеней. Но эффективной может быть только та учебная программа, которая нацелена на изменение менталитета, отношения людей к защите информации.

«Программа бесполезна, так как все равно найдутся разгильдяи, которые плюют на предосторожности и правила безопасности». Во-первых, безопасность не гарантирует 100% защищенность, но призвана минимизировать риски. Во-вторых, тренинги по защите информации – один из компонентов системы обеспечения безопасности бизнеса наряду с шифрованием, средствами обнаружения несанкционированных вторжений, антиспамовыми и антивирусными решениями. Тренинги ориентированы на человеческий фактор, который чаще всего становится причиной утечек данных и иных информационных проблем.

«Все и так знают, что надо делать». Автор утверждает, опираясь на собственный опыт организации тренингов в различных организациях, что подавляющее большинство сотрудников в компаниях не имеют и малейшего представления, что и как надо делать в случае вторжений и компрометации сетей. Проблема не в людях, а в том, как мы их обучаем.

«Главное – предотвращение рисков». Это очень важно, но не исключает обучение навыкам поведения, когда происходит вторжение или компрометация. Если вы, к примеру, имитируете попытку фишинга с целью проверить прочность защиты, то важно определить не только число потенциальных жертв, но и число тех, кто способен вовремя обнаружить атаку и сообщить, кому полагается.

«Да это очень просто». Это верно, если вы ограничиваетесь задачей ознакомить персонал компании с правилами информационной безопасности. Но если действительно желаете снизить риски через изменение отношения людей к этим вопросам, то надо иметь на руках продуманный план, предусматривающий, на кого рассчитана учебная программа, какие конкретно задачи ставятся, что ожидается на выходе...

Желающие могут ознакомиться с инструкциями по составлению планов тренинга, собственно учебными программами на сайте компании SANS Securing the Human (http://www.securingthehuman.org).

На охрану американских школ заступают вооруженные охранники

Серия массовых убийств в американских школах в последнее время вынудила учебную администрацию во многих штатах пересмотреть условия охраны в сторону ужесточения.

В городе Мальборо, штат Нью Джерси, в начале 2013 года в каждой школе появился вооруженный охранник. Мэр города Джон Хорник утверждает, что если раньше родители были категорически против присутствия охранников с оружием, то сегодня картина полностью поменялась. В дополнение, говорит мэр, рассматриваются перспективы использования новейших охранных технологий, изменений в проектировании учебных зданий.

Аналогичные и похожие новости приходят из многих американских городов. Исследование, проведенное недавно Security 500, показало, что наличие вооруженной охраны в школах успокаивающе воздействуют на детей и родителей. Последние

знают, что в случае инцидента именно профессионалы будут первыми, кто прикроет учеников.

Говорит Дуг Фогуэлл, старший вице-президент компании Allied Barton: «Охранники в школах - это отлично тренированные мужчины и женщины, обладающие набором профессиональных знаний и навыков – от способности находить общий язык с детьми до умения быстро и правильно реагировать на преступление. У них, как правило, за плечами немалый опыт работы в опасных ситуациях, задержания и обезвреживания преступников, пресечения деятельности криминальных банд, других противоправных действий» (Security Magazine, February 2013).

Эксперты обращают внимание, что охранники в школах тесно кооперируются с местными отделениями полиции, а многие из них раньше сами служили в правоохранительных структурах.

Как эти изменения скажутся на развитии охранной индустрии США? Организация Freedonia Group прогнозирует рост доходов в сфере частной охранной деятельности к концу 2013 года на 4.6%,. Они составят за год сумму 25 миллиардов долларов. Официальная статистика утверждает, что сегодня в США насчитывается более миллиона частных охранников.

Но у экспертов возникают вопросы, а все ли 1,033,000 американских специалистов охранного дела подготовлены одинаково на высоком уровне? Каковы назначение и роль охранника в униформе во внештатной ситуации? Может ли общественность быть уверенной, что охранник первым бросится под пули преступника? Нет никакой уверенности, что все профессионалы готовы в любой ситуации выбирать верные решения. Журналисты задают вопрос: скажем, в торговых центрах охранников учат оказывать первую медицинскую помощь, тушить пожар, стрелять на поражение в случае необходимости? Или их здесь держат, чтобы следить за магазинными воришками?

Что касается охраны школ, то и здесь возникает вопрос о полномочиях охранника. Должен ли он следить, чтобы ученики не курили в туалетах, не воровали по мелочи, не баловались наркотиками? Или его единственная задача – обеспечить защиту учащихся от внешних угроз? А будет ли он пресекать и другие возможные правонарушения? Дискуссии на эту тему идут сегодня по всей Америке.

(по материалам онлайнового журнала Security Magazine)

Канадский Форум профессионалов и партнеров в сфере корпоративной безопасности

Точное название этой организации – Canadian Security Partner’ Forum (сокращенно CSPF). Это общенациональная общественная организация, объединяющая разные структуры, каждая из которых представляет собой ассоциацию профессиональных охранников, офицеров по безопасности, преподавателей, в общем, всех тех, кто

работает в сфере охраны, безопасности бизнеса или смежных областях.

Основатель и бессменный председатель Форума - Грант Леки, который начинал карьеру рядовым охранником и дослужился до престижной должности руководителя отдела по вопросам защиты бизнеса в экстремальных условиях Управления гражданства и иммиграции Канады.

В интервью журналу Security Management (February 2013) он рассказывает, что в процессе своей служебной карьеры, которая, в частности, включала и научно-теоретический аспект (master degree), испытывал неудовлетворенность тем, как в Канаде ведется подготовка и обучение охранников, их денежным содержанием и общественным статусом. Одна из проблем, привлекшая его внимание, – разобщенность внутри индустрии безопасности, мешающая распространению удачных примеров, успешного опыта работы профессионалов. Некоторым из многочисленных объединений (ассоциаций) охранников явно не хватало «свежей крови», побуждающей рост профессионализма.

Так Грант Леки пришел к идее создания структуры, которая бы объединила разные ассоциации, служила бы механизмом обмена опытом, методологическим инструментарием, копилкой знаний обо всем, что происходит в охранной отрасли и смежных областях в национальном масштабе. Эту идею при поддержке коллег ему удалось реализовать через образование в феврале 2012 года CSPF. Сегодня в Форум входят 106 разных ассоциаций и союзов, представляющих индустрию безопасности во всех провинциях Канады. Форум развивает сотрудничество с такими международными организациями как ASIS (Международная ассоциация индустрии безопасности) и AESRM (Ассоциация по вопросам управления рисками, связанными с охраной и безопасностью предприятий).

Отвечая на вопрос корреспондента: «Какие свои качества вы считаете ключевыми как лидера?», Грант Леки заметил, что в начале своей карьеры он внимательно изучал, как работают окружавшие его более опытные и умелые коллеги. «Но быть хорошим лидером – это также способность видеть перспективы и уметь подбирать людей, помогающих трансформировать перспективы в реальность».

По традиции журнала, интервьюируемый рассказал, чем занимается в свободное время – чтение литературы, катание на велосипеде, туризм и путешествия.

Basic Private Investigation: A Guide to Business Organization, Management, and Basic Investigative Skills for the Private Investigator.

Basic Private Investigation: A Guide to Business Organization, Management, and Basic Investigative Skills for the Private Investigator.
By William F. Blake, CPP. Charles C. Thomas Publisher, 320 pages

Книга рассчитана на тех, кто, имея опыт работы в правоохранительных органах, вышел в отставку и собирается начать вторую карьеру в качестве корпоративного

расследователя. Это, конечно, далеко не единственный информационно-учебный источник по вопросам расследований, но читатель найдет в книге для себя много полезного.

Первый раздел посвящен начальному этапу карьеры в данной сфере. Среди рассматриваемых аспектов – правовые, маркетинговые, финансовые. Очень важна психологическая готовность бывших госчиновников окунуться в частный сектор экономики. Особенность новой для них сферы деятельности, в частности, состоит в том, что нередко внутрикорпоративные расследования проводятся без стремления обязательно наказать виновника, передав дело в руки полиции или в суд. Такие особенности надо учитывать, прежде чем принимать решение о начале новой карьеры.

Во втором разделе книги речь идет о базовых знаниях и навыках, необходимых для этой работы. Например, о том, как планировать расследование, как докладывать о результатах. По мнению рецензента, Росса Булла, президента компании The Treadstone Group, автору книги следовало бы больше внимания уделить отчетам, так как именно по ним клиент судит о квалификации и компетентности расследователя, и сократить главу, посвященную международным расследованиям, так как последние заслуживают отдельной книги.

В конечном счете, читатели получают глубокое представление о расследованиях как о профессии, о том, как делать успешную карьеру в этой области. В тексте имеются контрольные вопросники (checklists), образцы отчетов, истории и примеры из живой реальной практики.