Охрана предприятия

№4 (38), 2014

Оглавление

Лидерство

Важнейшие профессиональные компетенции в современной информзащите

Новые технологии, методологии

Технологии безопасности для банков

Экономика и финансы

Пять вещей, которые необходимо знать о страховании кибербезопасности

Риски и угрозы безопасности бизнеса

Охрана предприятия с помощью бэкграундных фильтров

Как не отстать от новых технологий и рисков в сфере обращения кредитных карт

Лицензия на воровство

Офисные окна как фактор риска

Рекомендации специалиста

Некоторые фундаментальные основы охраны учреждений здравоохранения

Безопасность отеля: как создать баланс гостеприимности и безопасности

К вопросу об увольнениях квалифицированных специалистов в сфере охраны предприятия

Как выбирать новую систему безопасности

Профессиональное образование и работа с кадрами

Тренинги персонала по безопасности: как это делать и делать лучше

Охрана предприятия за рубежом

Влияние национально-культурных особенностей на корпоративную безопасность

Книжное обозрение

Eavesdropping Surveillance & Espionage: Threats, Techniques & Counter-Measures

Countering Fraud

Исследования

Компании теряют в среднем 5% своих доходов в результате злоупотреблений персонала

Важнейшие профессиональные компетенции в сфере информзащиты

Редакция журнала Chief Security Officer провела опрос руководителей охранных предприятий, аналитиков и экспертов, представителей рекрутинговых агентств, чтобы понять, какие профессиональные знания и навыки сегодня наиболее востребованы в области защиты информации. Выделены следующие сферы этой индустрии:

Мобильные средства безопасности

Компании по всему миру во все большей степени полагаются на использование мобильных носителей информации, которые, однако, несут с собой новые для бизнеса уязвимости и угрозы. Спрос на специалистов, знающих, как надо противостоять этой опасности, сегодня растет не по дням, а по часам. В качестве технических средств защиты предлагаются программные решения, автоматизирующие контроль и аудит корпоративных сетей. Чтобы ими управлять, надо иметь специальные инженерные знания, умение кодировать и прочие навыки, позволяющие гарантировать безошибочную эксплуатацию новейших технологий информзащиты. Но именно здесь, в области программных продуктов безопасности, отмечается дефицит специалистов. Их подготовка не поспевает за быстрым развитием информационных технологий, в том числе и программ по безопасности мобильных носителей.

Аналитика данных

Эксперты сходятся во мнении, что здесь более всего нужны специалисты, разбирающиеся, помимо своей профессии, в особенностях экономики/бизнеса. Обладая аналитическими способностями, они успешны в отслеживании не только бизнес тенденций в данной отрасли, но также рисков и угроз, в определении степени их приоритетности и опасности для бизнеса, в обнаружении закономерностей и взаимосвязей между отдельными явлениями и фактами.

Анализ безопасности

В том, что касается компетенций специалиста по охране предприятия, то сегодня наиболее востребованы аналитики, способные управлять процессами интеграции соответствующих технологий, их тестированием и эксплуатацией. Такой специалист не может ограничиваться знаниями исключительно своей профессии, но должен разбираться в бизнес процессах компании, где он работает, понимать, какая информация наиболее ценна и заслуживает первоочередного внимания с точки зрения ее защиты. Он/она также обладает способностями отслеживать и идентифицировать активность киберпреступников и агентов промышленного шпионажа, анализировать информацию о рисках из разных источников.

Защита программных приложений

Поскольку компании все чаще принимают на вооружение веб-приложения, растет спрос на специалистов в области их защиты, которые способны минимально сокращать разрыв между новыми бизнес технологиями и средствами их защиты (последние, как правило, отстают от первых). С точки зрения руководителя службы безопасности наибольший интерес представляют эксперты, обладающие навыками разведки и обнаружения новых угроз и рисков.

(продолжение в следующем выпуске журнала)

Технологии безопасности для банков

Часть 2 (начало см. журнал №37)

Отделения банков фокусируют внимание на средствах физической охраны (тревожная сигнализация, пожарная сигнализация, анти-скимминговые устройства в банкоматах, камеры видеонаблюдения), в то время как для центров хранения данных первостепенное значение имеет информационная защита. За последние 15 лет, говорит Л.Чиапетта, директор по технологиям компании Protection 1, оба вида безопасности в значительной мере интегрируются с помощью «умных систем», заменивших компьютерами телефонные линии в физической охране (securitymagazine.com, April 1, 2014).

Все большее применение находят мегапиксельные камеры слежения, позволяющие идентифицировать злоумышленника.

С другой стороны, совершенствуются программные решения, далеко превосходящие по своим возможностям традиционные межсетевые экраны (firewalls), способные отслеживать взаимоотношения между участниками трансакций, выделять и фиксировать подозрительные сделки, странности в поведении финансовых игроков. Такие системы предупреждают о повышенной активности преступных групп в киберпространстве.

Другая сфера новых технологий – «облачные исчисления», завоевавшие огромную популярность у множества компаний, но в последнюю очередь – у банков и прочих финансовых организаций. Э. Йорад, глава компании Vaultive, отмечает, что «облака» - единственная инновационная сфера за последние 20 лет, где банки далеко отстали в

ее освоении от других бизнес индустрий, поскольку серьезно опасаются за сохранность своих данных. Так, одна из глобальных кредитно-финансовых организаций, тесно сотрудничающая с Vaultive, полагает, что одно дело, когда допуск к административным серверам компании имеют 4-5 человек, и совсем другое, когда таким допуском обладают сотни людей, использующие «облачные» исчисления, которые переданы в распоряжение стороннего провайдера.

Еще одна проблема «облаков» связана с вмешательством государственных органов управления. Многие «облачные» хранилища данных в своих корпоративных политиках связаны обязательством раскрывать информацию надзорным ведомствам в определенных случаях. «Банки задают себе простой вопрос: если третья сторона («облако») может раскрыть наши данные без нашего разрешения, то кто же тогда является действительным владельцем этих данных?», - отмечает Йорад.

Чтобы гарантировать себя от утраты контроля над корпоративной информацией, Йорад советует банкам постоянно прибегать к шифрованию данных – в процессе их обработки и отправки, любом другом использовании. Есть «золотое правило»: кто контролирует ключи от шифра, тот контролирует данные.

Второй по величине в Бразилии государственный банк Caixa Economia Federal отказался от традиционных пин-кодов как инструмента идентификации. Банк обратился к новейшей мультиспектральной технологии отпечатков пальцев. Три с половиной тысячи банкоматов оснащены устройствами, считывающими как поверхность пальцев, так и подкожную структуру. Второй, «внутренний» рисунок в отличие от поверхности пальца не подвергается воздействию влаги, грязи, одежды, а, следовательно, дает более надежную картину идентификации по сравнению с традиционными способами.

Пять вещей, которые необходимо знать о страховании кибербезопасности

Онлайновый журнал Chief Information Officer (CIO) опубликовал статью Л. Константина о страховании кибербезопасности

Такое страхование позволяет компенсировать, хотя бы частично, материальные потери в случае успешной атаки на корпоративные сети и базы данных, пишет автор. Но это далеко не полное решение возможных проблем. Надо иметь в виду следующие моменты:

1. Кибербезопасность представляет собой высоко рискованную стратегию

Страхование в пользу страхователя (first-party insurance) обычно распространяется на ущерб, наносимый непосредственно цифровому имуществу, а также в результате вынужденной приостановки бизнеса, реже в случаях репутационного урона. Страхование перед третьими лицами, т.е. клиентами компании (third-party insurance), подразумевает покрытие компенсаций, а также расходы на расследование,

оповещение клиентов, связи с общественностью, защиту в судах. Кибератаки настолько разнообразны и изощренны, что в реальности невозможно предусмотреть и гарантировать защиту от всех рисков подобного рода. Наилучший подход – определить наиболее ценные электронные данные и принять меры к их надежной защите.

2. Рынки в США и Европе различаются

Рынок страхования кибербезопасности в США более развит, чем в Европе. Страхование перед третьими лицами наиболее распространено в Америке, а страхование в пользу страхователя характерно для Европы. Рынок в США растет быстрыми темпами, примерно, на 30% в год в крупных компаниях, а в среднем на 10%.

3. Необходимо четкое обозначение границ страхования

Прежде чем подписывать контракт со страховой компанией, внимательно изучите, какие риски уже застрахованы, дабы не допустить частичное наложение одних на другие, а, следовательно, лишние расходы.

4. В некоторых сферах покрытие неадекватно

Страхование кибербезопасности, как правило, не позволяет полностью возмещать потери от кражи интеллектуальной собственности, репутационного урона, а также падения доходов (замедления темпов бизнеса) вследствие кибератаки.

5. Недостаточная мотивация для усиления кибербезопасности

В идеале страхование кибербезопасности должно стимулировать компании к совершенствованию систем защиты. На деле же страхователи не могут профессионально судить о том, какие продукты и системы контроля наиболее эффективны в защите информации конкретной компании и, соответственно, побуждать клиентов к выбору того или иного варианта страхования.

Охрана предприятия с помощью бэкграундных фильтров

Часть 1

Американская статистика свидетельствует, что при устройстве на работу 88% соискателей лгут в представляемых ими резюме. Один из примеров: проверка кандидата на руководящую должность в одной компании выявила растрату на прежнем месте работы в полмиллиона долларов. Понятно, в резюме этого кандидата о факте мошенничества ни словом, ни намеком (журнал Security Magazine, May, 2014).

Бэкграундная проверка – неотъемлемая часть процесса приема на работу. Очень часто эта функция выполняется совместно с кадровым отделом и службой безопасности, нередко с привлечением юридического департамента компании. Необходимость взаимодействия объективно обусловлена сложностью, объемностью стоящей задачи, которая включает верификацию квалификации и компетенций соискателя, его

практического опыта работы, проверку возможной связи с криминальным миром, фактов нарушения правил и норм корпоративной безопасности, что в свою очередь нередко требует обращения к архивным данным на государственном, региональном и местном уровнях. Если все названные службы работают независимо друг от друга в решении этой задачи, то высока вероятность ошибки, просмотра существенных деталей. В рамках же совместной их работы служба безопасности играет роль самого важного института проверки, несущего главную ответственность за адекватность результатов реальному положению дел.

Хорошим подспорьем в этой работе служат технологии, позволяющие интегрировать средства бэкграундного сканирования с программами рекрутирования, которыми располагает кадровый департамент, а также с электронными системами СКУД. К примеру, софт, отвечающий за контроль доступа, может быть отрегулирован таким образом, чтобы электронный пропуск для новичка (или временного работника, или представителя партнерской организации), не был активирован ранее, чем завершится процесс проверки.

Согласно опросу «2014 Benchmarking Report», только 15% респондентов, представителей разных компаний, сказали, что проводят глобальное бэкграундное сканирование для проверки квалификации и поиска криминальных следов соискателя, имеющего опыт работы за рубежом. Впрочем, в крупных компаниях процент вдвое выше.

Наибольшую потенциальную опасность представляют работники, не входящие в постоянный штат организации (временные, по срочному контракту, представляющие смежников, партнеров и поставщиков,...). Их, как правило, вообще не проводят через отдел кадров, но приглашают на работу от имени отраслевых подразделений, таких как отдел ИТ, департамент маркетинга, бухгалтерия. Их нередко находят с помощью рекрутинговых агентств, полагаясь на рекомендации последних. Но и в таких случаях главная ответственность лежит на службе безопасности, которая обязана проследить, чтобы никто не получал электронные пропуска на предприятие до завершения необходимой проверки.

Некоторые организации практикуют периодическую проверку уже принятых и работающих сотрудников, чтобы минимизировать долгосрочные риски путем контроля служебных и внеслужебных связей персонала. Согласно тому же отчету «2014 Benchmarking Report», этим занимаются всего 20% опрошенных компаний.

При общем признании необходимости и важности проверки на алкогольную и наркотическую зависимость, как в процессе приема, так и после зачисления на работу, только 58% респондентов сказали, что их компании такие проверки осуществляют. Между тем, очевидно, что речь идет не только об эффективности и продуктивности сотрудника, но и о серьезных рисках безопасности.

(продолжение в следующем выпуске журнала)

Как не отстать от новых технологий и

рисков в сфере обращения кредитных карт

Авторы публикации в журнале Security Magazine Джерри Бреннан и Линн Мэттис бьют тревогу, отмечая резкий рост преступности в сфере кредитных карт, обусловленный кибервторжениями в эту сферу.

Главной причиной авторы называют нежелание компаний-производителей и ритейлеров тратиться на пин-коды и микросхемы защиты. Мотивация – слишком дорогое удовольствие регулярно менять микросхемы и внедрять новые технологии в терминалы.

Авторы публикации с такой позицией не согласны. Они утверждают, что средства, затраченные на эти цели, полностью окупаются в течение одного, максимум двух лет. В тех странах, где активно внедряются новые охранные технологии, уровень преступности, связанной с кредитными картами, падает многократно.

Хакеры постоянно совершенствуют свое преступное ремесло, активно ищут и находят слабости и уязвимости. Таким слабым звеном предстают небольшие предприятия, участвующие в посреднических или снабженческих операциях. Понятно, что крупные корпорации могут позволить себе тратить сопоставимо большие средства на безопасность, в то время как многим их смежникам, представляющим малый бизнес, такие расходы не по карману. Они-то и есть то самое слабое звено, которое нередко служит хакерам порталом для вторжения в «святую святых» избранных жертв – корпоративную сеть.

Другая проблема, на которую авторы советуют обратить внимание, заключается в том, что компании не поспевают за появлением новых технологий. За этой сферой либо плохо следят, либо вовсе ее не отслеживают. Лишь очень немногие компании имеют в своем штате квалифицированных специалистов, которые осуществляют пристальный мониторинг инновационных изобретений, появления технологий, способных менять правила рыночной игры, а, следовательно, позволяющих их компаниям вовремя подготовиться к внедрению и управлению этими технологиями в ущерб менее расторопным конкурентам.

Авторы полагают, что не только компании обязаны следить за инновациями. Появление в восьмидесятые годы технологии «стелс» во многом обесценило традиционные системы радарного слежения. Что, в свою очередь, простимулировало появление более совершенных систем противовоздушной обороны.

В конце публикации авторы напоминают изречение, приписываемое Александру Македонскому: «Простительно проиграть сражение, но не простительно быть застигнутым врасплох».

Лицензия на воровство

Компания Fellows, Inc. занимается производством шредеров (машин для уничтожения бумажных документов), ламинирующих машин и другого офисного оборудования. В середине нулевых годов компания открыла совместное предприятие в Китае. Спустя некоторое время у партнера, китайской фирмы Shinri, сменилось руководство. Новые владельцы выдвинули к Fellows ряд требований, в частности, уступить право собственности на технологию предприятия. Когда компания Fellows отказалась, китайцы заблокировали производственные мощности, присвоили себе уже выпущенную продукцию, перевели счета предприятия в подконтрольный банк. Более того, подали в местный суд иск с целью легализации захвата всей собственности СП, как физической, так и интеллектуальной.

Эту историю рассказала на страницах журнала Security Management М. Гейтс. Люди обычно себе представляют торговые секреты как «нечто овеществленное», пишет автор, к примеру, рецепт приготовления кока-колы. Но сегодня к числу коммерческих тайн относятся также и специализированные программные продукты, и стратегически важная корпоративная информация, и методологии анализа, позволяющие из массы данных извлекать только то, что необходимо для принятия решений, и многое другое не вполне материальное.

В цифровую эпоху украсть бизнес секреты стало намного легче, так как компании хранят данные в своих сетях, подвергаемых хакерским атакам. Проблема усугубилась характерной для развитых стран тенденцией выводить производства в другие регионы мира. По данным International Trade Commission, утечки экономических секретов в Китае ежегодно обходятся американским компаниям в общую сумму более миллиарда долларов.

Основным средством борьбы с кражами секретов остаются апелляции в суды. Но местные суды, как правило, берут сторону соотечественников. В международных арбитражах можно надолго увязнуть без больших шансов на успех.

Том Статлер, руководитель службы СБ компании Raymond James, считает, что компаниям, потенциальным жертвам экономического шпионажа и рейдерства, следует занять более активную позицию в защите собственных секретов.

Сначала необходимо разобраться, что считать в компании коммерческой тайной. Такого рода аудиты надо проводить ежегодно, так как бизнес процессы постоянно меняются. Затем следует определить меры по защите и проконтролировать их неукоснительное осуществление.

Некоторые из таких мер довольно просты. К примеру, рекомендует Статлер, надо обеспечить в офисах «чистые столы», хранить, держать конфиденциальные документы в сейфах, по меньшей мере, в закрытых ящиках письменного стола.

Также необходимо проводить политику повышения осведомленности персонала относительного того, что следует считать коммерческими секретами и как надо их защищать. Такая программа (awareness program) должна охватывать всех сотрудников компании и получать поддержку со стороны топ-менеджмента.

В статье упоминается официально утвержденный госдепом США список стран, наиболее опасных с точки зрения промышленного шпионажа. В списке нашлось место и для России. Планирующим поездки в эти страны западным предпринимателям и менеджерам рекомендуется проявлять повышенные меры осторожности. В частности,

вычищать с мобильных девайсов информацию, которая может интересовать конкурентов, не оставлять компьютеры вне своего зрения, и так далее. Некоторые американские компании практикуют смену мобильных устройств после возвращения сотрудников из заграничной поездки, дабы обезопасить себя от возможных «жучков» и прочих вредоносных вещей, которыми гаджеты незаметно для их владельцев могут быть заражены.

Офисные окна как фактор риска

Боб Брэгдон, автор заметки на сайте csoonline.com (June 24, 2014), из гостиничного номера в Нью-Йорке, где он находился в командировке, мог свободно наблюдать, что делается в здании напротив, которое занимает крупная юридическая корпорация. Через огромные, от пола до потолка, стеклянные, не зашторенные окна он видел, как сотрудники корпорации проводят совещание в конференц-зале, как они работают, сидя за компьютерами, как общаются друг с другом.

Если бы автор заметки имел при себе сильный бинокль, то смог бы без труда заглянуть в лежащие на столах бумаги, прочитать содержимое экранов мониторов. А со специальным оборудованием – подслушать, о чем там совещаются.

Если бы на его месте, фантазирует автор, были конкуренты, или журналисты расследований, охочие до чужих секретов, то утечка информации, возможно, чрезвычайно важной, была бы неизбежной. Вывод из этой истории: проявлять бдительность, не забывать, что за вами могут подглядывать и подслушивать, используя ваше пренебрежение к таким, казалось бы, простым вещам, как ничем не защищенные окна.

Брэгдон дает несколько советов:

• Никогда не устанавливайте офисные доски, мониторы компьютеров лицом к окну; лучше расставлять их с ориентацией на боковые по отношению к дверям и окнам стены;

• Если вы проектируете для себя офисное помещение, предусмотрите работу персонала в комнатах, выходящих окнами на внутренний двор или на свободное от строений пространство;

• Используйте «слепые» или затененные оконные стекла; могут подойти и зеркальные, но надо помнить, что их эффективность снижается, когда за окном темнеет, а внутри включают свет.

• Постоянно напоминайте свои сотрудникам, что они могут попасть под «микроскоп»; тренинги по повышению осведомленности необходимы, но они дают эффект, если проводятся регулярно и настойчиво.

• Следите за тем, чтобы ничего не оставалось на столе, на экранах мониторов, на офисной доске по завершении работы или во время перерыва.

• Если офис расположен на первом этаже, важно предусмотреть, чтобы никто не мог

воспользоваться в злоумышленных целях окружающим здание природным ландшафтом (к примеру, использовать кусты как прикрытие для наблюдения).

Некоторые фундаментальные основы охраны учреждений здравоохранения

Журнал Security Magazine в майском выпуске за этот год опубликовал материал, посвященный вопросам охраны поликлиник и больниц. Автор статьи, Клэр Мейер, указывает, что любые учреждения в системе здравоохранения обязаны создавать и поддерживать атмосферу открытости и дружелюбия, но при этом не забывать о фундаментальных правилах и нормах безопасности. Каждый день идут потоки людей с разными целями: прием к врачу, сдача анализов, посещение пациента больницы, приобретение лекарства. Каждодневно по разным помещениям передвигаются работники лечащего и обслуживающего персонала. Практически невозможно за всеми усмотреть, проконтролировать каждый их шаг. Но необходимо соблюдать меры предосторожности, позволяющие до минимума свести всевозможные риски. Вот некоторые из них:

• Оснастить приемные, офисы, кафетерии и прочие помещения системой электронных ключей, управляемых дистанционно, а также электронными пропусками (соответственно и считывающими устройствами), ограничивающими пребывание гостей и пациентов по времени и территориально.

• Установить компоненты СКУД на лестницах и в лифтах, чтобы ограничить перемещение пациентов и посетителей с этажа на этаж. К примеру, разместить в лифтах специальные считыватели.

• Предусмотреть свободный доступ к запасным выходам в случае чрезвычайной ситуации.

• Постоянно контролировать, чтобы все двери функционировали, нормально открывались и закрывались.

• Отучать персонал от привычки подпирать и держать дверь открытой.

• Обеспечить нормальную работу раздвижных дверей (обычно используемых на входе и выходе внешнего периметра).

• Предусмотреть обязательную регистрацию с указанием цели визита посетителей, отметку при их выходе из учреждения.

• Установить систему видеонаблюдения в реальном времени и архивацией видеоданных. Это необходимо, в частности, для расследований инцидентов безопасности, а также для контроля за работой и поведением сотрудников учреждения.

• Предусмотреть везде, где необходимо, указатели. Это важно, чтобы посетители не забрели ненароком туда, где им быть не положено.

Безопасность отеля: как создать баланс гостеприимства и безопасности

Б.Шартие, вице-президент компании Alliedbarton Security Services, в статье, размещенной на сайте csoonline.com (June 23, 2014), делится своими соображениями о балансе гостеприимства и безопасности в отелях. Он предлагает следующие рекомендации:

Добиваться, чтобы обслуживающий персонал гостиниц ни на минуту не забывал о проблемах безопасности

Особенно это важно для охранников на входе и работников рецепции. Не «вестись» на роскошный лимузин и чемодан от Гуччи, не верить на слово, но в любом случае проверять наличие гостевой карточки или ключей от номера. Всегда проверять документы, прежде чем выдавать новые ключи вместо «потерянных».

Постоянно контролировать исправность, проверять на уязвимости системы электронных карт-ключей

На одной из конференций по вопросам безопасности хакер продемонстрировал слабости подобной системы, выпускаемой крупной компанией и используемой примерно для семи миллионов гостиничных номеров по всему миру. С помощью некоторых компьютерных устройств и не самой сложной программы он получил доступ к контролю системы электронных ключей. Владельцы компании-производителя немедленно отреагировали, начав работу по совершенствованию защиты.

Ввести постоянно действующий протокол бэкграундной проверки персонала

Ежегодные проверки сотрудников обеспечивают не только высокий качественный уровень, но и способствуют укреплению безопасности отеля.

Установить круглосуточный контроль доступа

Контроль доступа не должен ослабевать в то время суток, когда поток клиентов уменьшается или временно прекращается. Если клиент видит, что и поздно ночью, и ранним утром охранники не спят, они на своем рабочем месте, то у него/нее растет уверенность, что никакой злоумышленник в номер не вломится.

Обеспечить сочетание атмосферы гостеприимства и высокой безопасности

Создание и поддержание правильного баланса достигается опытом, специальной тренировкой, постоянным контролем со стороны руководства. При найме на работу охранники должны проходить тщательную проверку, не только бэкграундного свойства, но и на способность вежливо и умело общаться с клиентами.

Установить контакты между частной охраной и правоохранительными органами

В полицию часто обращаются по мелким вопросам, например, когда в ресторане отеля буянит пьяный клиент, или в номере слишком шумно отмечают встречу с друзьями…Тесное партнерство охраны отеля с местными полицейскими необходимо, в

частности, для того, чтобы разгрузить полицию от незначительных инцидентов, позволить ей сконцентрироваться на борьбе с преступностью. Но для этого в гостиничной охране должны работать высококвалифицированные специалисты, умеющие поддерживать – формально или неформально – контакты с полицией.

Иметь в наличии и по необходимости корректировать план реагирования на инциденты безопасности

Такие планы надо подвергать ревизии, по крайней мере, ежегодно при участии как можно большего числа людей из обслуживающего персонала. Важно, чтобы все работающие в отеле посещали тренинги по обеспечению безопасности, особенно в зонах лобби, рецепции, камеры хранения багажа, лестниц и коридоров, автопаркинга, короче везде, где высок трафик гостей.

К вопросу об увольнениях квалифицированных специалистов в сфере охраны предприятия

Постоянный автор онлайнового журнала Chief Security Officer Микаэл Сантарканжело обратил внимание на рост числа специалистов охранного дела, желающих поменять место работы, перейти в другую организацию.

В одном из объявлений он прочитал, что две трети СБ некой компании ищут новую работу. В этой связи он задает вопрос: насколько готовы компании расстаться с квалифицированными охранниками, офицерами по безопасности и что им надо делать, чтобы удержать сотрудников?

Для любого руководителя (и глава службы безопасности здесь не исключение) существует три категории подчиненных:

- кому нравится работа и не планирует переход в другую организацию;

- хотят уйти, но могут остаться по ряду причин;

- точно уйдут, рано или поздно.

Зная о намерениях коллег, важно понять мотивацию, чем обусловлено желание поменять место работы или, напротив, не менять ничего. Для этого необходимо ответить на следующие вопросы:

• Какую роль играет используемая в компании система поощрения и вознаграждения в формировании тех или иных намерений?

• Имеют ли сотрудники право голоса в принятии решений, прислушивается ли начальство к их мнению?

• Удовлетворительна ли система обучения и тренингов с точки зрения перспектив профессионального и карьерного роста?

Многое, подчеркивает автор материала, зависит не от материальных стимулов, а от общей атмосферы, в которой работают люди, от корпоративной культуры. В надлежащих условиях вряд ли возможна высокая кадровая ротация. Но если кто-то уходит, то, скорее всего, на более привлекательные условия.

Как часто бывает, реальная ценность сотрудника для компании обнаруживается, как только он ее покидает. Поэтому так важно проанализировать роль и функции каждого работника, чтобы понять, кого компания теряет в случае увольнения. Взвешивая личные достоинства и недостатки, необходимо выстраивать работу коллектива таким образом, чтобы результаты в меньшей степени зависели от отдельных людей, но в целом от командной работы.

Когда в коллективе начинаются разговоры о неудовлетворенности работой, о желании поменять организацию, самое время организовать с коллегами серьезный и откровенный разговор. О последствиях потери ключевых работников для охраны предприятия. О том, что надо сделать для улучшения условий работы. Как повысить роль и ответственность каждого члена команды за результаты работы. О реальных профессиональных и карьерных перспективах.

Такие обсуждения способствуют укреплению коллектива. Но и в случае увольнения каких-то работников, для компании это не будет сюрпризом, она сможет подготовиться.

Как выбирать новую систему безопасности

Рано или поздно перед каждой организацией встает вопрос об обновлении систем корпоративной безопасности. Как принимается решение о выборе той или иной системы? Какие шаги необходимо последовательно предпринимать? Кто должен участвовать в этом процессе? На эти и другие смежные вопросы отвечает Ким Рэхфалд на сайте securitymagazine.com.

Многие компании, оказавшись в такой ситуации, предпочитают приглашать эксперта для консультации в ходе всего процесса. Эксперты проводят тестирование на предмет выявления слабостей и уязвимостей организации с точки зрения ее безопасности, помогают в написании и корректировке соответствующих политик, процедур, плана закупки, по существу принимают участие в реализации плана.

Следующий шаг – рассылается запрос на информацию об имеющихся на рынке системах. Речь идет о производителях и поставщиках, качестве выпускаемой ими продукции, корпоративной философии, культуре обслуживания клиентов, ценовой политике и т.п. Не существует стандарта запроса. В нем могут быть и десять вопросов, и все сто.

Компании совместно с консультантами изучают все полученные ответы и сужают список до 3-4 фирм, с каждой из которых проводятся интенсивные переговоры, а также знакомство с реальными продуктами. В ходе демонстрации системы уточняются детали, касающиеся продуктов и их производителей/поставщиков.

В принципе покупатель может по согласованию с контрагентом поставить у себя систему на испытательный срок, чтобы досконально изучить ее работу, пригодность для организации всех ее функций: идентификация и верификация, тревожная сигнализация, видеонаблюдение...

Одновременно формулируется предложение для системных интеграторов, специализирующихся в данной отрасли экономики. Последние предоставляют подробную информацию о себе и отобранном продукте. Разрабатывается проект контракта на работу по установке системы с указанием стоимости материалов и работ.

Покупатель вправе установить контакт с теми организациями, которые уже используют данный продукт, поинтересоваться, насколько он их устраивает, соответствует ли тому, что обещал производитель/поставщик, можно ли систему модернизировать по прошествии определенного времени, насколько продавец/поставщик готов выполнять функцию долговременного партнера, поскольку система обычно предназначена для длительной, 10-15 лет, эксплуатации.

После всех этих процедур принимается окончательное решение с учетом оптимального соотношения цены и качества, надежности системы, а также доверия к поставщику.

Тренинги персонала по безопасности: как это делать и делать лучше

На сайте csoonline.com 16 июня 2014 г. размещена статья Т. Армединга о проблемах, связанных с тренингами персонала компаний по безопасности. Автор отмечает, что человеческий фактор выступает самым слабым звеном в охране предприятия. А между тем, как показывают опросы, более половины компаний вообще не проводят занятия со своими сотрудниками по вопросам безопасности.

Недавний отчет EMA (Enterprise Management Associates – основанная в 1996 году исследовательская и консалтинговая организация) дал такие результаты:

- треть персонала (33%) опрошенных 600 компаний использует одни и те же пароли для офисных и собственных девайсов;

- 35% признались, что открывают письма незнакомых корреспондентов;

- почти две трети хранят информацию в «облачных исчислениях»;

- почти столько же хранят конфиденциальные данные компании на своих мобильных устройствах.

К сожалению, многие компании не видят смысла в проведении занятий с персоналом в рамках «программы повышения осведомленности» (awareness program). Часто это объясняется слабым качеством самих программ, даже если они и есть в наличии. Такая форма тренинга как семинары с упором на монологи, сходные с лекциями, не дает должного результата, отмечают эксперты.

Говорит Дж.-Л. Хеймерл, старший стратег по безопасности компании Solutionary: «Эффективная программа повышения осведомленности имеет мало общего с презентацией концепций безопасности. Ее цель – привить сотрудникам новые навыки и привычки, отвечающие задачам безопасности».

При этом огромную роль играет индустриальный профиль компании. Что хорошо для банков, возможно, не будет работать применительно к сфере здравоохранения.

Имеет место быть фаталистическое убеждение, отмечает Хеймерл, что затраты времени и денег на такие тренинги обесцениваются при малейшей оплошности кого-то из работников, ошибочно, случайно кликнувшего на вредоносную ссылку. Да, такое может быть. Но цель программы – минимизировать подобные риски.

Все же в отношении персонала компаний к тренингам по безопасности происходят позитивные сдвиги. Отвечая на вопрос, что им представляется наиболее важным относительно обучения, 66% ответили: «доступность в понимании», а 61% - «легкость в использовании рекомендаций на практике».

Организация Information Security Forum (независимая ассоциация по вопросам информационной защиты) выработала рекомендации по изменению поведения и мышления персонала компаний в правильном направлении. В частности, предлагается:

- помогать работникам осознавать важность мер предосторожности;

- добиваться, чтобы такие меры были понятными и легко усваиваемыми;

- мотивировать, в том числе материально, верные решения;

- не приказывать подчиненным, а вырабатывать правильные привычки;

- разработать и осуществлять политику поощрений и наказаний.

Влияние национально-культурных особенностей на корпоративную безопасность

Как считают многие американские эксперты, США отстают от других стран в уровне обеспечения охраны предприятия. Это касается как физического периметра безопасности, так и финансовой, информационной защиты. Иногда такое расхождение в подходах объясняют различиями в национально-культурной сфере разных народов.

Билл Бессе, вице-президент по консалтингу и расследованиям компании Andrews International, пожил в Стамбуле и отмечает, что все более-менее значимые здания оборудованы магнитометрами, сканерами, x-ray устройствами. Каждый посетитель подвергается тщательному досмотру, но при этом все относятся к мерам безопасности спокойно, словно это часть привычной, повседневной жизни. Такую же ситуацию Бессе наблюдал в некоторых других странах. В Индии после атаки террористов в Мумбаи

(2008 г.) во всех крупных торговых центрах и отелях круглосуточно дежурят вооруженные полицейские, частные охранники, повсеместно используются магнитометры. В Израиле сканирование автомобилей, проверка их водителей и пассажиров при подъезде к торговым центрам и другим местам скопления людей – обычное, рядовое явление.

А, скажем, в Японии ситуация совершенно иная. Эрик Милам, управляющий компанией Accuvant, по заданию клиентской фирмы испытал на прочность охрану принадлежащих клиенту складских помещений в Японии. Преодолеть периметр безопасности оказалось проще пареной репы. Тестирование проводила команда из двух американских парней, не знающих ни слова на японском языке. Прибыв в страну, они обнаружили редкостное дружелюбие и гостеприимство местного населения. Никто не удосужился прямо их спросить: «А что вы здесь делаете?».

Никакой особой подготовки несанкционированного проникновения на территорию складов не предполагалось. Заранее были отпечатаны фальшивые бэджики-пропуска, составлено вымышленное письмо от имени несуществующей американской компании с просьбой допуска в офис. Когда американцы вылезли из мерседеса у входа в офис, никто их ни о чем не спрашивал. Ни признака настороженности, ни пристального внимания к бэджикам. Сплошное радушие и дружелюбие. Гостей провели в офис.

Иногда и фальшивые пропуска не нужны. Милам вспоминает, как, проводя аналогичную операцию на нефтеперерабатывающем комбинате в Нидерландах, он не смог преодолеть СКУД. Тогда на следующий день, который оказался выходным для многих работников предприятия, он подошел к проходной, где познакомился с курившей неподалеку женщиной. Он рассказал даме, что «его босс внезапно должен сегодня улететь по срочному делу, а человек, с которым он связан, сегодня не работает, но надо забрать некоторые документы». Женщина легко поверила, подвела к охраннику и попросила пропустить. Охранник, ни слова не говоря, провел «гостя» через СКУД на территорию предприятия.

Милам также упоминает, как однажды в Испании попытался пройти на совещание одной организации, подделав письмо и подпись главного юриста этой компании. Охранник, женщина средних лет, однако, наотрез отказалась его впускать в конференц-зал. Но поскольку посетитель продолжал настаивать, женщина показала «письмо» одному из руководителей совещания, который в жесткой форме потребовал пропустить гостя. Милам характеризует этот эпизод как проявление чисто национальной культуры испанцев, где традиционно «мужчины привыкли повелевать женщинами».

(по материалам журнала Chief Security Officer, June 23, 2014)

Eavesdropping Surveillance & Espionage: Threats, Techniques & Counter-Measures

Eavesdropping Surveillance & Espionage: Threats, Techniques & Counter-Measures
By Norbert Zaenglein; Reviewed By Paul D. Barnard, CPP

Night Howl Productions; modernprivacy.info; 246 pages; $59

Как отмечает автор книги, если до недавнего времени изощренное шпионское оборудование было доступно только крупным организациям, то сегодня миниатюризация средств подслушивания и подглядывания, их высокое качество, потенциал передачи данных на расстояние представляет собой реальный вызов для множества компаний и людей.

Книга охватывает широкий спектр вопросов и проблем, связанных с борьбой против промышленного шпионажа. В частности, речь идет о методологии обнаружения электромагнитных устройств, акустических девайсов, шпионских камер слежения, средств нейтрализации тревожной сигнализации, способов слежения с помощью GPS технологии, перехвата кабельных и беспроводных коммуникаций, проникновения в компьютерные сети. Отдельная глава посвящена методам физического контроля и разоблачения шпиона.

Книга отлично обеспечена визуальным рядом - фотографиями, рисунками, таблицами.

Информативное содержание издания рекомендуется как профессионалам корпоративной безопасности, так и студентам.

Countering Fraud

Countering Fraud
By Mark Button and Jim Gee; Reviewed By Sandy Gosselin, CPP
Wiley.com; 208 pages; $60

Книга представляет собой руководство по созданию и осуществлению программы противодействия хищениям в компании. Авторы в деталях рассказывают о необходимых компонентах такой программы. Используют статистику там, где это необходимо.

Важно, что в книге подробно анализируются проблемы, связанные с обращениями компаний в правоохранительные и судебные органы. Хотя авторы основываются на опыте Великобритании, книга полезна всем компаниям, в какой бы стране они ни находились. Каждый, намеревающийся разработать эффективную программу борьбы с хищениями, найдет здесь для себя много полезного, отмечается в рецензиях.

Компании теряют в среднем 5% своих доходов в результате злоупотреблений персонала

Такой вывод следует из исследования, проведенного Association of Certified Fraud Examiners («Объединение сертифицированных специалистов по борьбе с хищениями» – международная некоммерческая профессиональная организация, в 2007 году открыт

филиал в Российской Федерации).

Средние годовые потери от хищений оцениваются в сумму почти $150 000. В каждом пятом случае (из общего числа взятых 1 500 фактов в ста странах мира) ущерб достигает миллиона долларов.

При этом характерно, что, как правило, на воровстве попадаются сотрудники, ранее не подозревавшиеся в преступных намерениях. 80% злоумышленников совершили хищения впервые, проработав не один год в компании. Две трети из них – мужчины.

85% преступлений связаны с растратой: подделка документов по командировочным расходам, проведение зарплатных ведомостей для уже уволенных сотрудников, фальсификация инвойсов и осуществление переводов на подставные фирмы. Но обычно такие виды злоупотреблений не оборачиваются крупными финансовыми потерями.

Наибольший урон наносят представители руководящего звена, разрабатывающие и осуществляющие схемы увода денег. Хотя они составляют всего 19% от общего числа раскрываемых преступлений, средний от них ущерб составляет полмиллиона долларов.
Для сравнения – обычный сотрудник в среднем совершает хищение на сумму 75 000 долларов.

Три четверти всех преступлений совершают работники бухгалтерии, операционисты, управленцы среднего и высшего уровня, а также менеджеры, работающие непосредственно с клиентами, поставщиками, смежниками.

Там, где хищения осуществляются группой лиц, потери, как правило, выше, чем урон, наносимый индивидуумами – от 200 до 500 тысяч долларов.

Если брать отдельные отрасли экономики и бизнеса, то наиболее уязвимыми с этой точки зрения являются финансовые услуги, государственные заказы, производство. Именно здесь раскрывается наибольшее число преступлений. А самые высокие средние потери от воровства отмечены в горнодобывающей индустрии, сфере недвижимости, углеродном сегменте.

Наиболее эффективными методами борьбы с хищениями, подчеркивается в отчете, считаются хорошо отлаженная система стимулирования информаторов (попросту говоря, «стукачей») и четкий мониторинг данных.