Охрана предприятия

№2 (36), 2014

Оглавление

Руководитель службы безопасности в 2014 году

Журнал Chief Security Officer провел очередной опрос среди руководителей корпоративных служб безопасности. Некоторые результаты и выводы:

Спрос на таланты все еще превышает предложение

Эксперты обращают внимание, что многие организации делают упор на внедрение новых технологий безопасности, испытывая при этом дефицит человеческого интеллекта, аналитического потенциала. Компании жалуются, что не могут подыскать нужного им специалиста в этой области, несмотря на высокие заработки руководителей соответствующих подразделений. Большинство глав корпоративных СБ в США зарабатывают в год порядка 180 000 долларов. Это в среднем. В крупных корпорациях зарплата может достигать 235 000 долларов. В сравнительно небольших организациях колеблется между 140 000 и 150 000 долларов. Несмотря на эти цифры, дефицит высокопрофессиональных специалистов стоит довольно остро.

Директоров по безопасности больше всего беспокоят (в порядке убывающей значимости): а) мобильные носители; б) хакерские атаки; в) осознание персоналом значения безопасности и кооперация в этой сфере.

Компании уделяют повышенное внимание киберугрозам, как извне (56%), так и изнутри (34%). Эксперты подчеркивают, что минимизировать риски на этом направлении следует путем более глубокой интеграции вопросов безопасности в процессы принятия бизнес решений.

Офицеры по безопасности стали чаще и сильнее влиять на принятие решений топ-менеджмента.

Примерно три четверти опрошенных отметили, что за последний год стали тратить больше времени на встречи с первыми лицами и другими представителями высшего звена компаний, консультируя и представляя рекомендации по вопросам охраны предприятия. Это положительный тренд в борьбе руководителей СБ за место за столом, где принимаются решения. Офицеры по безопасности выходят из тени и все чаще напрямую докладывают и контактируют с первыми лицами.

Более трезвый взгляд на технологические аспекты

Данный момент связан, в первую очередь, с модой на «облачный» аутсорсинг. При

всех очевидных преимуществах этого направления растет осознание потенциальных угроз. Многие приходят к выводу, что любой аутсорсинг, в том числе «облачный», всегда риск. На вопрос о продуктах безопасности 75% респондентов ответили, что довольны самими продуктами (производителями), но только 64% - сервисными службами. Между тем, отмечается, что наиболее опытные офицеры безопасности полагают неверным чрезмерный акцент на чисто технологические аспекты их работы в ущерб вниманию борьбы с реальными противниками в лице криминала, злоумышленников. Похоже, что восторженность и увлеченность чисто техническими аспектами идет на спад. Еще одна проблема заключается в том, что многим руководителям в сфере корпоративной безопасности не хватает технического образования. Из-за этого они с трудом находят общий язык со специалистами в информационных технологиях.

Основные направления развития физической охраны

Старший редактор журнала Chief Security Officer опубликовал статью, посвященную наиболее актуальным сегодня проблемам физической охраны. Главная особенность последних лет – интеграция с информационными технологиями. Тенденция объективная и положительная, однако, несущая с собой новые риски и угрозы.

Бэджики RFID (радиочастотной идентификации)

Эти электронные пропуска, получившие сегодня широкое распространение, содержат два вида информации: код веб-сайта и персональные данные. Они уязвимы, поскольку не имеют защиты против хакеров, аналогичной той, которую используют компании для защиты корпоративных сетей, практически не реагируют (просто не замечают) на хакерские атаки. К тому же некоторые организации передают свои системы RFID «облачным» провайдерам, что ничуть не усиливает их защиту.

Видеонаблюдение

Совершенствование технологий видеонаблюдения вышло на уровень практического использования методов лицевого распознавания (facial recognition). Мегапиксельные камеры дают отличное изображение. Вместе с тем, остается большим вопросом пропускная способность беспроводных систем, особенно при наличии большого числа камер.

Системы охраны периметра

Достижения в этой области восхищают экспертов. Особенно выделяют использование микроволновых и радиоволновых технологий, сигнализирующих о приближающихся к периметру объектах, что дает возможность своевременно отреагировать на потенциальные угрозы.

Распознавание по радужной оболочке глаз

Хотя преступники разрабатывают средства преодоления этой защитной методологии с

помощью искусной технологии фотографии, пройти безнаказанно биологический барьер чрезвычайно сложно.

СКУД

Несмотря на развитие современных технологий безопасности человеческий фактор (работа охранника) не становится менее значимым, хотя подчас и недооценивается теми, кто все надежды возлагает исключительно на автоматизированные системы охраны. Остаются проблемы, где машины не способны заменить опытного и внимательного охранника. Например, в случае, если кто-то пытается пройти по чужому (в том числе электронному) пропуску.

Безопасность, замкнутая на мобильные носители

Сегодня уже никого не удивишь мобильными устройствами, с помощью которых можно осуществлять контроль за системами безопасности, управлять домашним хозяйством, открывать и закрывать дверные замки. Одновременно с удобством приходят и уязвимости. Люди, пользующиеся многофункциональными смартфонами и айфонами, обычно ограничиваются самыми простыми решениями защиты девайсов, например, функцией блокировки в случае потери или кражи. Это иногда выручает, но в долгосрочной перспективе требуются более надежные средства защиты от злоумышленников.

Сканирование отпечатков пальцев

Эта технология пока еще далека от совершенства. К примеру, отпечатки пальцев могут быть скопированы с помощью специальных желатиновых материалов. Об этом известно производителям продуктов безопасности. Некоторые приступили к изготовлению и выпуску таких устройств, которые помимо фиксирования рисунка пальца одновременно улавливают уровень температуры, а также распознают структуру вен.

Распознавание по лицу

Соответствующие технологии сегодня используются широко, в частности, в отслеживании потоков пешеходов для поиска конкретных разыскиваемых лиц. Вместе с тем, как полагают некоторые эксперты, имеющиеся в продаже верификационные системы пока не очень надежны. Они нередко ошибаются при схожих очертаниях лица разных людей. А, кроме того, злоумышленник, зная о подобных технологиях, может легко маскироваться (наклеивать усы, бороду), или просто надвигать на лоб мягкую шляпу. Так что впереди еще долгий путь совершенствования данной технологии.

Семь полезных привычек эффективного офицера безопасности

(по материалам сайта csoonline.com)

1. Коммуникабельность

Б. Уильямс, исполнительный вице-президент Sysnet Global Solution: Коммуникабельность – важнейший элемент профессионала в сфере корпоративной безопасности. В этом залог успешной или неудачной карьеры. Можно досконально разбираться в своей специальности, но если вы не в состоянии толково рассказать о своей работе бизнесменам, убедить их в ее важности, то вас просто уже не пригласят для консультаций.
Б.Мартин, основатель Digital Trust: слабые коммуникационные навыки – следствие образования в школах, где от тебя требуют только прилежания и усидчивости. Этим отчасти объясняется, почему многие профессионалы уходят с головой в детали своей работы, игнорируя или, по меньшей мере, недооценивая роль контактов с коллегами и начальством.

2. Сообразительность в вопросах бизнеса

Знание бизнеса компании не менее важно, чем знание своей прямой специальности. Оно необходимо, чтобы уверенно чувствовать себя, встречаясь с руководителями, коллегами из профильных бизнес подразделений, убеждать их в необходимости поддержки функции безопасности.
Б. Свердлик, менеджер технологий безопасности компании Tagged: Когда вы приходите работать в организацию, то первым делом надо вникнуть в вопросы бизнеса, понять, как зарабатываются деньги, каковы риски и угрозы бизнесу.
Б. Уильямс: Немалое значение имеет склонность к компромиссам. Мы (работники в сфере корпоративной безопасности) нередко говорим «нет» новым веяниям, не давая себе труда разобраться в плюсах и минусах инноваций с точки зрения своей профессиональной позиции. В одной компании директор по безопасности запретил персоналу приносить на работу мобильные носители, не понимая, что все равно сотрудники, особенно молодежь, будут пользоваться в рабочее время собственными девайсами, но скрытно от руководства.

3. Креативность

Необходимое качество, в частности, для разрешения технических проблем.

4. Аналитические способности

М.Мартин: Никто не может сказать, что он (она) знает все на свете. В процессе работы постоянно приходится сталкиваться с новыми, ранее неизвестным, иногда даже странными проблемами, решать которые невозможно, не владея глубоким, «корневым» анализом.

5. Жажда новых познаний

Необходимо быть в курсе новостей, новых тенденций в правовом поле применительно к охране предприятия, в сфере технологий безопасности, в других вопросах, связанных с профессией. К примеру, за последние 5 лет многие технологии изменились до неузнаваемости. Информацию можно черпать в океане ресурсов, включая книги, блоги, социальные сети, новостные сайты. Следует один - два раза в год участвовать в конференциях и форумах.

6. Участие в бизнес проектах компании

Совместная работа в проектах и программах компании дает возможность всем

участникам лучше понимать друг друга, находить общий язык, в частности, в вопросах охраны предприятия.

7. Знать приемы и методы злоумышленников

Важно уметь представить себя на месте потенциального хакера или иного преступника, и с этой позиции внимательно проанализировать все аспекты охраны предприятия, выявить слабости и уязвимости, заблаговременно их устранять, минимизируя риски.

Служба безопасности и контрактники: работа одной командой

Когда у компании дела идут неважно и приходится сокращать расходы, нередко под нож попадает служба безопасности. Часть штатных сотрудников увольняют, нанимают охранников по контракту. К аутсорсингу также прибегают для проведения разовых мероприятий. Бывает, между постоянными и временными работниками возникает недопонимание, даже неприязнь. Теме взаимоотношений СБ и охранников по контракту посвящена одна из публикаций февральского выпуска журнала Security Magazine.

Боб Каверман, помощник президента учебного заведения Columbia College по вопросам безопасности, утверждает, что никаких разночтений, а, тем более, разногласий между собственной службой безопасности и 75 контрактниками не существует. Все работают как одна команда. Это достигается, прежде всего, отлаженным процессом отбора и найма. Помимо традиционных процедур проверок, Каверман с коллегами проводит углубленные собеседования с кандидатами, пытаясь понять, насколько они коммуникабельны, представительны внешне, пригодны для специфической работы в городском студенческом кампусе.

После зачисления на работу, охранникам Columbia College предстоит осуществлять широкий спектр функций – патрулирование (пешком, в автомобиле, на велосипеде), дежурство в командном центре, работа с видеонаблюдением, системами СКУД, средствами тревожной сигнализации и массового оповещения, и т.д. Охранники прикреплены к конкретным постам. Студенты к ним привыкают. Охранник, в свою очередь, обретает способность заметить и оценить те или изменения на вверенном ему участке. Так контрактники осваивают специфику, постепенно врастают в единую службу безопасности.

Ким Клавайтер трудится директором по безопасности профессионального футбольного клуба Minnesota Vikings. В дни игр он координирует работу 600 охранников по контракту, которые выполняют самые разные функции: от проверки содержимого сумок, с которыми зрители приходят на соревнование, до проверки входных билетов на стадион. Когда игр нет, службу несут несколько патрулей на территории стадиона. Для выездных игр приходится нанимать контрактников для охраны автобуса, автомашин игроков и болельщиков (число машин, сопровождающих клуб, доходит до 150-200). Клайватер работает с одной и той же охранной фирмой на протяжении ряда лет, поэтому полностью доверяет тем, кого ему отправляют на день-

два работы.

Майк Джонстон – региональный директор по безопасности транспортно-посреднической компании DSC Logistics and Supply Chain Management. Статистика краж на транспорте, говорит он, свидетельствует, что чаще всего преступления совершаются на перевалочных складах. Поэтому особое внимание уделяется хранению грузов. Некоторые клиенты, владельцы грузов, сами диктуют, какую охранную фирму выбрать для найма контрактников. Но чаще выбор остается за DSC. Джонстон лично проводит селекцию фирмы, изучая предложения, ведя переговоры. Выбор падает на компанию, где хорошо поставлена кадровая работа, где регулярно проводятся тренинги. Джонстон сам проводит расследование криминальных инцидентов. Программа работы с контрактниками строится как собственная служба безопасности, поглощает массу времени и усилий, требует хорошей организации. В конце концов, все усилия оправдываются хорошими результатами. И доходами.

Технологии на защите репутации

На сайте securitymanagement.com опубликована статья под заголовком “Reputation Protection”, характеризующая некоторые технологии мониторинга, с помощью которых можно отслеживать, контролировать и влиять на имидж и репутацию компании в прессе и социальных путях.

По данным одной из консалтинговых фирм, 92% пользователей Интернета знакомятся с отзывами других потребителей о продуктах и услугах. 89% признались, что мнения покупателей влияют на их выбор. В этом одна из причин, почему компании так заботятся о том, как они выглядят в интернете – онлайновых обзорах, чатах, блогах, других видах социальных медиа. Анализируя данные, можно почерпнуть немало важной информации о репутации компании. Кроме того, обнаружить подделки своей продукции. Вот некоторые из поисковых машин, которые помогут в мониторинге.

Truckur

Пользователь выбирает ключевые слова и закладывает в поисковый процесс. Машина просматривает отраслевые сайты, социальные сети, блоги. Если возникают проблемы с отслеживанием какого-то сайта, в распоряжении пользователя технология RSS (веб-агрегатор, позволяющий транслировать практически любой материал с любого сайта).

Ключевыми словами обычно являются название фирмы, его продуктов, ФИО руководителей и менеджеров, …Машина не только отыскивает и отбирает упоминания о компании, но и систематизирует информацию в автоматическом режиме по эмоциональным или иным заданным параметрам в категориях «положительно», «отрицательно», «нейтрально».

Пользователь имеет возможность ответить (также автоматически) на то или иное упоминание, отправить пост на сайт или электронный почтовый ящик. При этом вся интерактивная переписка фиксируется и записывается.

Компании, использующие Truckur, вносят месячную плату: $27 за пять поисковых операций, $97 за 50 операций. Полный пакет услуг обходится в сумму $447 в месяц.

MarkMonitor

Особенность этого продукта – нацеленность на обнаружение контрафакта. В фокусе мониторинга – страницы онлайнового маркетинга, реклама, посты в социальных сетях. Технология предусматривает возможность немедленной реакции, в частности, в виде требования о снятии материала, которое направляется на сайт, где информация обнаружена.

RepTrak

Патентованная система под названием «модель RepTrak» активно используется крупным международным бизнесом, например, для оценки репутации потенциального партнера. Первым делом технология позволяет получить информацию о владельцах, акционерах. Затем проводятся фокус группы и интервью с потребителями продуктов. Как правило, звучат такого рода вопросы: «вы доверяете компании, в какой степени?», «вам нравится компания?», «ваши чувства по отношению к компании?», «вы уверены в хорошей репутации компании?». Ответы обрабатываются в автоматическом режиме. Оценка выражается в баллах от 0 до 100.

Эксперты по вопросам корпоративной репутации выделяют 7 основных критериев оценки: продукты и услуги; инновации, офисные и/или производственные помещения; управленческое звено; гражданская позиция (например, относительно экологии); стиль руководства; финансовые показатели.

Мобильные тревожные кнопки в системе охраны больниц

Насилие – не такое уж редкое событие в больницах и госпиталях, отмечает Эрик Смит, директор по безопасности крупного госпиталя в городе Денвер: 565 больничных коек, 18 500 пациентов в год плюс 169 000 посетителей амбулаторного лечения. Персонал госпиталя - 4 850 человек, не считая нескольких сотен волонтеров.

В интервью журналу Security Management (February 2014) Смит подчеркивает, что большинство инцидентов не носят серьезного характера (хотя случаются суициды), но в любом случае никто из врачей и медсестер не хочет рисковать получить синяк под глазом.

Некоторое время назад служба безопасности внедрила технологию мобильных тревожных кнопок (panic-button system). Именно мобильных. Большинство предлагаемых на рынке систем предусматривают кабельные стационарные технологии, где используется внутренняя телефонная сеть с центральным пунктом приема. Прокладывать кабели через больничные палаты и прочие помещения посчитали делом затратным и мало эффективным. В этом смысле принятая на вооружение система мобильных устройств Radius Enterprise Mobile Duress отличается в выгодную сторону. Во-первых, она беспроводная, работает с помощью ретрансляторов. Во-вторых, в случае инцидента не нужно вспоминать, где находится ближайшая тревожная кнопка. Она всегда при враче/медсестре. В-третьих, стационарная система предполагает 2-минутный разрыв между подачей сигнала и его получением службой безопасности. Мобильная система сокращает разрыв до 20

секунд. Трансляторы работают на батарейках, заряд которых рассчитан на 24 часа. Подзаряжаются от любой электророзетки.

У координатора системы нет привычных компьютера и монитора. Сигнал поступает в «умный» сервер, который определяет место и посылает сообщение ближайшему от места происшествия охраннику одновременно в разных форматах: на мобильник, пейджер, по электронной почте, а также через двустороннюю радиосвязь на мобильный приемник/передатчик.

Систему можно настроить таким образом, чтобы все сигналы поступали в диспетчерскую охраны.

Для минимизации случайных, ложных сигналов устройства снабжены двумя кнопками. Сигнал уходит при одновременном нажатии обеих кнопок в течение секунды.

Врачи и работники госпиталя получают устройства перед дежурством и носят все время с собой. После работы возвращают. С персоналом проводятся тренинги, где обучают и инструктируют, как обращаться с кнопками. После первого занятия выяснилось, что не все поняли и разобрались. Для таких проводится дополнительный тренинг.

Система уже продемонстрировала свою надежность. Произошел инцидент в комнате оказания первой медицинской помощи: пациент попытался покончить с собой. Медсестра включила устройство и через 30 секунд подоспела охрана. Пациента спасли.

Видеонаблюдение для малого бизнеса

Этой теме посвящена публикация в журнале Security Magazine (6 января 2014). Автор, Клэр Мейер, на примере ряда торгово-розничных предприятий рассказывает о тех преимуществах, которые получают предприниматели от использования систем видеонаблюдения, несмотря на их очевидную дороговизну и ограниченность бюджета мелких бизнесов.

Владельцы автозаправочной станции Warrior Fuel в штате Нью Мексико установили 36 камер наблюдения, включая бензоколонки, кассу, принадлежащие станции кафе и магазин, административный офис. Клиенты здесь расплачиваются обычно наличными, а потому «гляди в оба». Всякий неприятный инцидент изучается с помощью видеозаписей, которые необходимы при обращении в полицию или для тренинга персонала. Один из недавних примеров. Водитель отъехал, забыв убрать шланг из бака. Камера зафиксировала номер машины, поэтому не составило труда отыскать владельца и заставить оплатить причиненный ущерб.

Кривая убытков пошла вниз в магазине одежды в Des Moins. Лавка, ориентированная на молодежь и подростков, до недавнего времени несла убытки от воровства в размере более одного процента доходов. Установка 19 IP камер наблюдения снизила убытки почти наполовину. Один из методов, которые используют воришки - подмена ценовой бирки на другую, от более дешевого товара, в расчете на то, что продавцы не заметят. Теперь этот номер не проходит. Очень часто злоумышленники, чтобы не засветиться на мониторе, надвигают на лоб бейсболку и опускают голову, входя в

магазин. Администрация установила секретную камеру на уровне головы человека среднего роста. Записи при необходимости передаются в полицию, а также в общественную организацию торговцев «Группа по противодействию магазинных краж», которая собирает и хранит информацию о правонарушителях.

Семейный ресторан Redamark’s Tavern в Нью Буффало, штат Мичиган, увеличил количество камер с 9 до 30. В малом бизнесе поданная клиентом жалоба в суд может поставить предприятие на грань разорения. Видеонаблюдение помогает разоблачать непорядочное поведение некоторых алчных клиентов. Вот пример. Клиент подал в суд иск на ресторан, требуя 50 000 долларов компенсации за причиненный вред здоровью вследствие того, что «он поскользнулся на грязном полу и упал». Тщательное и непредвзятое изучение судом сохранившейся видеозаписи показало, что клиент просто разыграл падение. Видеонаблюдение помогает бороться с жуликами, пытающимися улизнуть, не заплатив за еду. Камеры также обозревают подходы к ресторану и паркинг.

В другом питейном заведении, суши баре Turk’s Seafood в городе Меттапойсетт (штат Массачусетс), более 20 камер видеонаблюдения помогают не только бороться с криминалом, но и контролировать работу персонала ресторана. Камеры отслеживают кассовые аппараты, кухню, входные двери, зал обслуживания, административные помещения. В любой момент управляющий баром может проверить, все ли служащие работают и правильно выполняют свои служебные обязанности, проследить, чтобы никто не воровал, чтобы клиентам не приходилось долго ждать своей очереди. С помощью камер проверяется, вовремя ли работники приходят на работу и уходят, что, естественно влияет на их заработки. Видеонаблюдение также выручает, когда клиент настаивает, что дал двадцать долларов, в то время как на деле всучил десятку. В итоге, заявляет владелец, с внедрением камер слежения убытки приблизились к нулю.

Новые технологии: в погоне за инновациями забывают о безопасности

Эксперты уже более 10 лет обращают внимание на отсутствие взаимосвязи между «умными» девайсами и вопросами безопасности. Такое положение чревато серьезными негативными последствиями, поскольку комфорт и удобства, создаваемые новыми, все более изощренными технологиями, могут быть сведены к нулю усилиями криминала. Практически все проблемы безопасности в этой сфере обусловлены распространением встроенных в «умные вещи» компьютерных систем, весьма уязвимых для хакерских атак.

Чем больше в мире «умных вещей», тем серьезнее угрозы. К примеру, по некоторым подсчетам, к 2015 году количество технологических продуктов, связанных с Интернетом, достигнет цифры 25 миллиардов. К 2020 году их уже будет 50 миллиардов на земном шаре. Если сегодня примерно 10% автомобилей имеют интернет платформы, то через 5 – 6 лет таких машин будет 90%. Уже сегодня потребительский рынок в изобилии предлагает нам устройства, которые следят за

нашим здоровьем, позволяют дистанционно управлять домашним хозяйством, делать кучу других умных вещей. Но практически все эти устройства несут значительные риски нашей безопасности, подчеркивают эксперты, которых проинтервьюировал журнал Chief Security Officer.

В Соединенных Штатах Федеральная торговая комиссия разработала рекомендации предусматривать элементы безопасности в производимых в стране смартфонах и прочих «умных» девайсах. Однако такие изделия скорее представляют собой исключения в мощном потоке выбрасываемой на рынок продукции. К. Хеффнер, специалист по компьютерным рискам компании Tactical Network Solutions, утверждает, что «потребительские девайсы практически лишены защиты, по меньшей мере, не отвечают современным стандартам безопасности». Проблема, по его мнению, в том, что рядовой потребитель, приобретая вещь, в последнюю очередь думает о безопасности, если вообще задумывается на эту тему.

Другой эксперт, Брюс Шнейер, главный технический офицер по безопасности в компании BT, пишет в своем блоге, что практически всё, что сегодня производится, от мобильных устройств до крупных инфраструктурных объектов, не имеет надежной защиты от хакеров. В этом, считает он, виноваты и потребители, и производители, но главным образом, последние. Чтобы обеспечить надлежащую защиту высокотехнологичных продуктов, нужны время и деньги. Большинство компаний не утруждают себя этими вопросами, поскольку потребители сами не задумываются над безопасностью, покупая смартфоны и прочие подобные изделия.

Такая ситуация будет продолжаться до тех пор, пока потребители в массе своей не почувствуют последствия легкомысленного отношения к технологиям, пока не обнаружат и не запаникуют от того, что хакеры с легкостью овладевают их банковскими счетами и электронными ключами от дома и автомашин.

Одна из отговорок производителей – дополнительные элементы защиты несут потребителям трудности в управлении, дискомфорт. Мол, если вы выпустите защищенный телевизор, который сложно включать и выключать, потребитель отвернется. Однако многие эксперты считают противопоставление удобства и безопасности «натянутым». Оба аспекта должны иметь приоритет при создании девайсов. Те производители, которые смогут определить и претворить в жизнь правильный баланс, в конечном счете, выиграют, и за ними будущее рынка «умных вещей».

Как уменьшить инсайдерские киберугрозы

Инсайдерство в сетях компаниях проявляет себя намного реже, чем хакерские атаки извне, отмечает Стивен Шабински, главный эксперт по рискам компании CrowdStrike на сайте securitymanagement.com (January 6, 2014). Зато убытки от каждого отдельного инсайдера потенциально выше, чем от внешнего хакера. Действуя изнутри, злоумышленники не только пользуются разрешенным доступом в сети. Они, как правило, в курсе уязвимостей информационной защиты, а, кроме того, знают, где

искать наиболее важную информацию.

Опасаться надо не только злоумышленников. Угрозу могут представлять и вполне благонамеренные сотрудники, допускающие утечки по небрежности, невнимательности, разгильдяйству.

Автор приводит некоторые статистические данные. В 85% случаев инциденты происходят по вине собственного персонала. Остальные 15% приходятся на счет партнеров и смежников. Главные цели инсайдеров – мошенничество (44%), кража интеллектуальной собственности (16%), саботаж (25%). Преступления обычно совершаются в рабочее время (72%).

Организациям рекомендуется иметь специальные программы, предусматривающие мобилизацию ресурсов, необходимых для того, чтобы предотвращать, вовремя обнаруживать и минимизировать риски. Помимо общей инструкции по информационной защите, такие специальные программы предполагают:

- тщательную проверку соискателей на работу в компании;

- инвентаризацию компьютерного имущества и аудиты с целью выяснить, как работники обращаются с офисной техникой;

- мониторинг трафика в сетях для выявления и исследования аномалий;

- контроль содержания сообщений, отправляемых из организации на онлайновые адреса и персональные аккаунты;

- отслеживание работы с офисными принтерами;

- контроль за мобильными носителями информации;

- надзор над сотрудниками, ранее замеченными в нарушении инструкций, выражающими недовольство компанией, добивающимися допуска к важной конфиденциальной информации, вызывающими подозрения иными неадекватными поступками.

- регулярный аудит привилегированных пользователей сетей, включая требование, чтобы по особенно важным проектам и заданиям работали не менее двух человек;

- меры, предусматривающие защиту информаторов от мстительных коллег;

- тренинги с персоналом, нацеленные на обнаружение инсайдерских рисков по конкретным признакам.

Малый бизнес: немногие обращаются в полицию

Проведенные в США исследования показывают, что владельцы и управляющие малыми предприятиями предпочитают не вмешивать правоохранительные органы во внутренние разборки с ворами.

64% малых предприятий, так или иначе, страдают от краж, совершаемых персоналом, но только 16% из них обращаются за помощью в полицию. 40% случаев связаны с кражей денег (в среднем 20 000 долларов). В остальных случаях покушаются на изделия, оборудование, офисное имущество.

По статистике удается схватить за руку злоумышленника лишь на 16-й месяц его/ее преступной деятельности. Кто эти люди? 20% - менеджеры, управленцы, остальные – мелкие служащие в бухгалтерии, рецепции,... Как ни странно, но кассиры составляют всего 2% уличенных в воровстве.

Автор этого исследования, Джей Кеннеди из университета Cincinnati, сформулировал четыре причины, почему мелкие предприниматели не хотят привлекать полицию:

1. Бизнесмен не считает, что угроза тюрьмы остановит воровство и чаще всего ограничивается увольнением.

2. Адвокат не советует обращаться в полицию, поскольку сэкономленные на судах деньги и время перевешивают сомнительные выгоды от посадки преступника.

3. Эмоциональный фактор: многие из тех, кого ловят за руку, имеют смягчающие обстоятельства – либо долго и с пользой работали в компании, либо находятся в родственных отношениях с владельцами.

4. Бизнесмены считают правоохранительную и пенитенциарную системы неэффективными и некомпетентными. Расследование финансового мошенничества требует специальных знаний, которых нет у обычных полицейских следователей. Поэтому вызванные на место преступления стражи порядка чаще всего ограничиваются общим отчетом. Кроме того, распространено мнение, что полиция должна заниматься более серьезными проблемами, чем офисное воровство.

(по материалам журнала Security Magazine)

Рекомендации для тренинга охранников по контролю за доступом (access management)

Эмми Тоубен – эксперт по предотвращению террористической деятельности. На сайте securitymagazine.com (6 января 2014) он предлагает свои рекомендации по тренингу охранников.

Он отмечает, что контроль за доступом требует особого внимания к человеческому фактору, который здесь «исключительно важен». Прежде всего, надо определить, где начинается этот контроль. Многие представляют себе контроль за доступом как непосредственное общение охранника с посетителем: проверка документа, вопросы-ответы, проверка списка гостей... Это необходимые компоненты контроля, но далеко не все.

Контроль начинается уже на подходе посетителя к входу в здание (помещение). В

идеале охранник должен располагаться таким образом, чтобы обозревать как можно большее пространство около охраняемого объекта. Его работа начинается уже в тот момент, когда он видит приближающегося посетителя. Он визуально оценивает клиента, что дает выигрыш во времени, позволяет действовать мгновенно, пока тот не приблизился вплотную.

В эти мгновения охранник должен оценить внешний вид (одежда, ручная кладь, и т.п.), а также «язык тела» (походка, манера поведения, и т.д.). Оценки должны соотноситься с конкретной обстановкой. В одном районе города, в определенной среде, такое поведение может показаться подозрительным, но в другом городском районе, даже поздно вечером, абсолютно нормальным. Поэтому инструкции и наставления надо тесно связывать с конкретными условиями предстоящей работы.

По мере приближения оценка становится более детальной и точной. Например, как ведет себя человек, спокойно или нервничает. Общие признаки нервозности: испарина, пот, бледность или, наоборот, красный оттенок лица, частота дыхания, сухость рта, нервное сглатывание слюны, выражение на лице тревоги, нетерпения.

Если хотя бы один из признаков беспокойства замечен, то охранник должен спросить себя, какие могут быть тому причины. Ответить на этот вопрос помогут большая спортивная сумка, дорогая итальянская обувь, «язык тела». Любая деталь может что-то рассказать. Понятно, что за несколько секунд невозможно создать сколько-нибудь полную картину, но их вполне достаточно, чтобы заранее подготовить правильные вопросы к посетителю.

Разговор желательно начинать с общего приветствия-вопроса: «чем могу помочь (быть полезен)?». Затем, в зависимости от ответа, задать целенаправленные вопросы. Если замечено, что ответ заранее заучен или сопровождается волнением, то можно обратиться с т.н. «глупым вопросом», например, о погоде. Вопрос звучит не к месту, но его не ждет собеседник, а потому отвечает обычно искренно, а, следовательно, лучше обнаруживает внутреннее состояние человека, его волнение, обеспокоенность…

При проверке личности охраннику важно иметь в виду несколько вещей. В первую очередь, помнить наизусть список возможных подделок в удостоверениях и документах (плохая ламинация, отслоение, вспучивание, несоответствие фото с реальным лицом или, напротив, нарочитое соответствие – в прическе, в одежде, например, тот же галстук, фото неправильно приклеено, множество прочих деталей, связанных с датами, числами, буквами, шрифтом и т.д.).

Сегодня на рынке много технических средств, помогающих обнаружить фальшивые документы. Во время проверки, если есть какие-то сомнения и подозрения, можно подвергнуть посетителя психологическому тесту. Например, затянуть время проверки, каждые несколько секунд поглядывая на клиента, как бы сравнивая его внешность с предъявленным фото на документе. Если тот действительно что-то скрывает, то обязательно обнаружит свое нетерпение. Можно, не торопясь, задать дополнительные, уточняющие вопросы, внимательно следя за реакцией. Есть и другие приемы, о которых рассказывают тренеры.

Автор публикации подчеркивает необходимость проведения подобных тренингов для овладения навыками сбора информации, развития наблюдательности и внимания к деталям, особенно к тем, которые вызывают подозрение. Здоровая доза скептицизма (подозрительности) – важный компонент эффективного контроля.

Как вести себя при устройстве на работу специалистом по информационной защите

Рекомендации экспертов собрал и обобщил журнал Chief Security Officer (January 15, 2014).

Продемонстрируйте привлекательные личностные черты. Вы можете быть гением в технических вопросах, но если произведете впечатление раздраженного, замкнутого, скованного человека, не умеющего расположить к себе, наладить нормальные взаимоотношения с коллегами, то едва ли получите работу в преуспевающей фирме.

Не только умно отвечайте, но и не менее умно задавайте вопросы. К примеру, такие вопросы: «С какими основными вызовами безопасности организация сталкивается?»; «Имеются ли планы расширения команды специалистов по безопасности?»; «Какие конкретно проблемы информационной защиты требуют неотложного, первоочередного решения?»….

Не производите впечатления всезнайки. Все прекрасно понимают, что человек, приходящий в организацию, не способен сразу же, с первого дня овладеть всеми деталями и нюансами новой работы. Требуется некоторое время. Поэтому не стоит создавать впечатление, что вы все знаете, все умеете, все вам по плечу. Такое поведение может насторожить представителей компании и негативно повлиять на решение.

Проведите предварительное исследование о компании и бизнесе, которым она занимается. Соберите хотя бы общую информацию о том, что происходит в данной отрасли экономики и бизнеса, каков стиль работы компании, ее культура, история, основные данные – размер бизнеса, количество офисов (филиалов), и т.п. Во время беседы используйте эту информацию, чтобы показать, что организация вас очень интересует.

Узнайте как можно больше о том, кто с вами будет беседовать. Как долго он/она работает в организации, технические знания, публикации или выступления в прессе, социальных сетях. Собранная информация поможет в поиске общих взглядов, подходов и даже хобби.

Оденьтесь соответствующим образом. В каждой компании своя культура работы и общения, включая стиль одежды. В одной компании принято быть застегнутым на все пуговицы и при галстуке. В другой – более либеральный подход. Если вам не удалось собрать такую информацию в СМИ, то перед встречей прямо спросите, как будет проходить собеседование – в галстуках или без.

Заранее изучите перечень должностных обязанностей и продумайте, насколько вы соответствуете требованиям. Это поможет вам сконцентрировать внимание только на тех вопросах, которые входят в должностные функции, избежать пространных разглагольствований о том, что вы умеете, если эти ваши возможности не имеют значения для будущей работы. При этом помните, что в большинстве случаев такой

перечень предполагает идеального, но не реального соискателя. Поэтому не смущайтесь, если соответствуете не на все 100%.

Готовьтесь к ответам на неудобные вопросы. Например, почему вы хотите переменить работу, что не устраивает в той организации, из которой уходите и т.п. Не надо вываливать сразу все грязное белье по поводу прежней или пока еще нынешней вашей организации. Высказываться на эту следует очень осторожно, нейтрально. Например, подчеркнуть, что вы стремитесь приобрести новый опыт, новые знания…

Корпоративная этика и безопасность

В тех компаниях, где поддерживается здоровая атмосфера, высокая корпоративная культура, внимание к вопросам этики является нормой, сама этика вплетена в ткань бизнеса, пишет в журнале Security Management (February 2014) специалист по этим вопросам Эрик Фелдман. Автор подчеркивает, что корпоративную этику следует рассматривать как важный элемент борьбы с мошенничеством и злоупотреблениями внутри организации.

Его вывод подтверждается рядом исследований. В частности, ученые установили, что компании, имеющие строгий кодекс корпоративной этики, вдвое меньше страдают от злоупотреблений персонала, чем компании, пренебрегающими такими документами. Речь идет не только о прямых финансовых убытках, но и о потерях репутационных, которые сложно перевести на язык долларов, но которые всегда и ощутимо влияют на конечные результаты.

Кодекс профессиональной этики, пишет автор, должен четко формулировать взаимные обязанности организации и сотрудников, включая обязанность работников сообщать начальству о замеченных случаях злоупотреблений, неправильного поведения, коррупции.

В реальной действительности требования этического характера очень часто напрямую противоречат финансовым, операционным и другим метрикам бизнеса, где выгода, прибыль – абсолютный приоритет. Погоня за финансовыми показателями, нередко завышенными, нереалистичными, вынуждает работников поступаться этическими принципами, нарушать нормы, прописанные в корпоративном кодексе.

Тем не менее, такой документ необходим. Автор рекомендует регулярно организовывать с персоналом занятия специально по вопросам корпоративной этики, хотя бы время от времени проводить аудит. В практическом смысле следование букве и духу кодекса должно защищать от ошибочных решений при найме новых сотрудников, продвижении (не всегда заслуженном) по службе, заключении партнерских отношений. Во время бесед с соискателями на работу в компании необходимо обсуждать этические дилеммы, чтобы выяснить отношение к ним кандидата. Выбор партнеров, поставщиков также должен учитывать уровень этической культуры.

Успех любой организации определяется не только финансовыми, материальными показателями. В атмосфере цинизма, равнодушия, недоверия вряд ли можно рассчитывать на большие рыночные достижения, утверждает автор статьи. Многое зависит от среднего звена управления, играющего ключевую роль в создании

здорового климата.

В большинстве компаний поощряется доносительство. В то же время эксперты фиксируют растущее неприятие такой формы противодействия мошенничеству и коррупции среди персонала. В частности, исследователи пришли к выводу, что почти каждый пятый из числа тех, кто хоть раз докладывал о злоупотреблениях коллег, испытывал на себе ненависть и месть. С другой стороны, нежелание разоблачать злоупотребления, как правило, обусловлено безразличием начальства.

Низкая этическая культура, в конечном счете, суживает возможности борьбы с коррупцией, усиливает риски для бизнеса.

Рецензии

The Successful Security Leader: Strategies for Success
by Harold Grimsle; amazon.com; 108 pages; $17.96; also available as an e-book

Автор книги, опираясь на собственный опыт работы директора по вопросам безопасности в трех крупных корпорациях, рассказывает, как ему удалось сделать удачную карьеру. Он пишет, что профессиональный успех обусловлен двумя взаимозависимыми факторами: личностными качествами и организационными способностями. Важно, чтобы офицер по безопасности не замыкался исключительно на своих прямых должностных, чтобы компания могла рассчитывать на него/нее в решении более широких задач бизнеса. Автор подробно излагает стратегию взаимоотношений внутри корпорации.

The Comprehensive Handbook of School Safety.
Edited by E. Scott Dunlap. CRC Press; crcpress.com; 454 pages; $119.95; also available as e-book.

Сборник статей посвящен широкому спектру проблем охраны школ: от организации контроля за доступом до управления форс-мажорными ситуациями. Каждый раздел сборника снабжен приложениями, ссылками на дополнительные источники информации, оставляет вопросы для дальнейшего обсуждения. Безопасность рассматривается в широком смысле, включает, в частности, противопожарную безопасность, охрану здоровья учащихся на транспорте, спортивных площадках, в столовой. Также излагается методология разработки и реализации планов по безопасности, в том числе и тренингов для персонала и школьников.

Security Consulting, Fourth Edition by Charles A. Sennewald, CPP. Elsevier/Butterworth-Heinemann; 264 pages; available at ASIS Online Store (www.asisonline.org); member: $55.00; nonmember: $61.00; item 2062

Четвертое издание фундаментальной книги по консалтингу в сфере охраны предприятия предназначено тем, кто хотел бы использовать свои знания, навыки и опыт практической работы офицером безопасности для перехода к консалтинговой деятельности. Автор книги предлагает воспользоваться его опытом профессиональной трансформации. Подробно излагаются и анализируются такие темы как

профессиональная квалификация, отвечающая требованиям консалтинга, этика, контракты и доходы, с чего начинать консалтинговый бизнес. Не забыты и такие вопросы как расследование финансовых махинаций, поимка магазинных воров. К основному тексту прилагаются образцы контракта по оказанию консультационных услуг, других документов.

США: бизнес стал уделять больше внимание защите приватной информации

Транснациональная консалтинговая корпорация PricewaterhouseCoopers провела исследование среди американских компаний на предмет их отношения к охране приватной информации (включая персональные данные) своих клиентов.

Главный вывод: значение защиты приватных данных возрастает, но недостаточно быстрыми темпами. К примеру, большинство из 370 респондентов заявили, что считают сохранение приватности клиентской информации «приоритетом среднего уровня».

Отношение к этой проблеме во многом определяется профилем бизнеса. В сфере финансов и медицины внимание к ней повышенное по сравнению с другими отраслями.

Среди менеджеров понимание значения privacy еще довольно слабое. 47% респондентов - членов правлений - заявили, что знают о privacy, но затруднились ответить на вопрос, как privacy влияет на деятельность их организаций. А 13% признались, что вообще не в курсе.

Одна из причин такой ситуации, считают авторы исследования, заключается в том, что большинство в верхнем звене управления ориентируется на внешние аспекты работы компании в ущерб анализу внутренних вопросов, к каковым относится защита приватной информации.

Многие путают безопасность и privacy. Они выслушивают доклады службы безопасности и считают, что этим исчерпывается вопрос privacy. Другие управленцы целиком полагаются на юридическую службу, которая, по их представлению, занимается этим вопросом (что далеко не так на деле). Все же исследование свидетельствует, что бизнесмены и топ менеджеры начинают постепенно разбираться в отличиях между охраной предприятия и охраной приватной информацией.

Одна из проблем заключается в обилии внутренних политик и инструкций, уследить за соблюдением которых чрезвычайно сложно. Компаниям необходимо разобраться, какие технологии, какие группы людей, какие управленческие проекты необходимо контролировать с точки зрения их соответствия внутренним политикам, не забывая о privacy.

Другая сложность для американских фирм порождена отсутствием законодательства и приватной информации на федеральном, общенациональном уровне. В каждом

штате собственная правовая трактовка. Отрасли также по-разному формулируют требования.

Но поскольку понимание важности этого вопроса среди бизнесменов все же растет, в ряде крупных компаниях вводят должность ответственного за охрану приватной информации – chief privacy officer.