Охрана предприятия

№1 (53), 2017

Оглавление

Системы контроля и управления допуском

Йельский Университет модернизирует систему СКУД

Рекомендации специалиста

Как защитить коммерческий сайт от мошенников, хакеров и ворующих торговые марки

Как обезопасить компанию с дистанционными сотрудниками

Создание условий для карьерного роста внутри компании

Книжное обозрение

The Guide to Online Due Diligence Investigations

Основные тренды в американской индустрии безопасности в 2016 году

Онлайновый журнал Security Magazine опубликовал 1 декабря 2016 г. обширный материал с анализом наиболее характерных тенденций последнего года в охранной индустрии США. Предлагаем вниманию читателей сжатые тезисы основных положений доклада.

Сначала немного статистики. В Америке в сфере негосударственной охраны работают 8□000 фирм, в них заняты в качестве постоянных штатных сотрудников 800□000 офице ров. Суммарный годовой доход – 43 миллиарда долларов. По данным на 2015 год среднечасовой заработок охранника по стране составлял 13.68 долларов или 28□460 долларов в год.

Ключевыми словами индустрии в 2016 году стали: консолидация, технологии, обучение и партнерство.

Консолидация

Самое крупное слияние произошло между Universal Services of America и AlliedBarton Security. Возник новый гигант Allied Universal с доходом 4.8 миллиардов долларов в год.

Рост индустрии, оцениваемый в 5% в год, сопровождается усиливающейся консолидацией через процессы слияния и поглощения. На примере Allied Universal это означает укрепление отделений по всей стране и за рубежом, уменьшение числа суб-контрактов, сокращение персонала, значительная экономия на аренде помещений,

приобретении и эксплуатации технологий.

Для меньших по размеру конкурентов такие слияния представляют как плюсы, так и минусы. Плюсы заключаются в том, что на местах многие клиенты предпочитают иметь дело не с обезличенными гигантами индустрии, но с конкретными местными специалистами. Им они психологически больше доверяют. Минус в том, что «крупняги» предлагают более разнообразный ассортимент услуг, и в этом небольшим кампаниям трудно с ними конкурировать.

С другой стороны, крупным клиентам, особенно транснациональным корпорациям, слияния на руку, им проще иметь дело с мощными охранными организациями.

Технологии

Здесь главную тенденцию аналитики видят в постепенном вытеснении роботами живой рабочей силы. Технологически вся отрасль подошла к важному рубежу, перейдя который, она будет стремительно насыщаться умными машинами, захватывающими всё новые охранные функции. Компаниям такой тренд выгоден. Сокращаются расходы на зарплаты, страховки, оплату бюллетеней и т.п. Кроме того, живым людям свойственно ошибаться, особенно в стрессовой ситуации. Идущие им на смену роботы лишены человеческих слабостей. Следовательно, и у начальства меньше головной боли.

Тори Броунярд, глава фирмы по страхованию охранной деятельности, вспоминает: «40 лет назад на ежегодном форуме ASIS 99% выставочных площадей занимали частные охранные фирмы. Сейчас 95% площадей принадлежат технологическим новинкам».

Обучение

Ускоренное технологическое развитие охранной отрасли существенно повышает требования к квалификации офицеров. И здесь обнаруживаются большие проблемы. Уровень подготовки охранников отстает от развития технологий безопасности. Эксперты отмечают, что обучение полицейского ведется сотни часов, прежде чем он может приступить к работе. А частных охранников нередко готовят за 8 часов, причем экзамен представляет пустую формальность.

Способностью управлять сложными технологиями не ограничиваются высокие требования. Охранник должен обладать коммуникационными способностями, уметь четко и грамотно сообщать об инцидентах, сохранять хладнокровие и ум в чрезвычайных ситуациях....

Партнерство

Огромное значение приобретает умение контактировать с клиентами и партнерами, среди которых - компании по производству технологий и правоохранительные органы.

Корпорация G4S, к примеру, установила тесные партнерские связи с клиентом в лице компании Expert Global Solutioins и местными отделениями полиции. Взаимодействие

дало отличное результаты. Один пример. Паркинг колл-центра Expert Global в рабочие дни заполняют порядка 1 200 – 1 500 автомобилей сотрудников (2 000 человек персонала) и посетителей. Каждый год случались десятки краж из машин. G4S ограничила въезд на паркинг, установив вокруг бетонные блоки, организовала патрулирование. В итоге кражи почти прекратились.

Какие просчеты приводят к увольнению офицера корпоративной СБ?

Постоянный автор журнала Security Magazine Джерри Бреннан отмечает в одной из своих последних публикаций, что смена руководителя корпоративной службы безопасности часто происходит, когда меняются владельцы или топ-менеджмент. Новые первые лица, проводя глубокую реорганизацию компании, решают, кто останется, а кто должен уйти.

Автор статьи приводит перечень ошибок, которые могут послужить основанием для увольнения офицера безопасности.

1. Недооценка значения кадров. Как бы вы ни относились к тем или иным своим подчиненным и коллегам, они являются интегрированной частью команды и требуют к себе уважительного отношения.

2. Неспособность работать слаженно в коллективе. Даже если вы способнее всех других коллег, успех приносит только дружная командная работа.

3. Пренебрежение имиджем. Какие бы замечательные идеи вы ни генерировали, не надо забывать о том, как они воспринимаются в коллективе.

4. Игнорирование иных точек зрения. Люди с диктаторскими замашками редко добиваются успеха в командной работе.

5. Неумение наладить отношения с руководством компании.

6. Слишком узкое видение и понимание проблем. Бизнесмены предпочитают работать с теми, у кого большой кругозор, кто хочет и умеет заглянуть за горизонт.

7. Безразличное отношение к клиентам компании. Это очень важный момент для общей оценки работы службы безопасности первыми лицами компании.

8. Замкнутость характера, отстраненность от коллег. Проблемы социальной коммуникабельности, противоречащие принятой в компании культуры общения, могут

стать причиной увольнения.

9. Неэтичные и противоправные действия. Звучит парадоксально для офицера службы безопасности, но такое случается, хотя и довольно редко (нарушения финансовой дисциплины, взятки и т.п.).

Банки: кибербезопасность и физическая охрана взаимно дополняют друг друга

Последние годы проблематика кибербезопасности смотрится намного актуальнее и острее вопросов физической охраны. Банковская сфера в этом отношении не исключение. Между тем, анализ инцидентов безопасности неопровержимо свидетельствует о тесной взаимосвязи обоих направлений.

Вот что по этому поводу говорит старший вице-президент Ассоциации американских банкиров Дуг Джонсон: «В наиболее выигрышном положении находятся те финансовые организации, которые добиваются высокой степени интеграции между тем, что они делают в плане физической охраны, и тем, что предпринимают в области кибербезопасности. И действительно: кибербезопасность имеет прямое отношение к современным технологиям СКУД, к девайсам, отвечающим за идентификацию людей в процессе контроля доступа к материальным средствам и инфраструктуре компании, включая инфраструктуру самой кибербезопасности» (Security Magazine, декабрьский номер за 2016).

С проектами по совмещению физических и кибер средств безопасности работает Микаэл Бэкон, управляющий партнер консалтинговой фирмы Resolvrizk: «Необходимо создать дружную, единую команду. Для этого требуется время и много усилий. Например, для организации тренировочных «настольных игр» с распределением ролей и ответственности. В принципе это не так сложно. Но мало кто серьезно этим занимается».

Один из объектов интеграции – банкоматы. Сочетание физической охраны и кибербезопасности необходимо, чтобы антискимминговые устройства, устанавливаемые в банкоматах, работали и не давали мошенникам свободы для маневра. Так, во всех 14 отделениях Банка Нью Гэмпшира банкоматы установлены в таких местах, где они находятся под постоянным наблюдением банковского персонала и любое неадекватное, подозрительное поведение немедленно будет отмечено. При этом с работниками банка регулярно проводятся соответствующие тренинги.

Другое важное для интеграции направление – электронные денежные трансферы, безопасность которых определяется как программными продуктами, контролирующими допуск и трафик в корпоративных сетях, так и традиционными техническими средствами физической охраны, ограничивающими доступ в служебные помещения.

Еще одна точка пересечения – электронные компоненты СКУД, в частности, видеокамеры и считыватели карт-пропусков. Все они требуют надежной защиты от

хакеров. Многие компании обзавелись цифровым видеонаблюдением и системами электронного доступа, но только со временем обнаружили, что эти высокие интернет технологии представляют собой заманчивый для хакеров объект атаки.

То же самое можно сказать и об «интернете вещей». Многие работники финансовой сферы накупили себе девайсы для дистанционного управления «умным домом», не подозревая, что собственноручно создают канал, по которому хакеры не только легко «проникают» в дома, но и пользуются малейшей возможностью через домашнюю сеть пролезть в корпоративные данные.

(продолжение в следующем выпуске)

Технологии, позволяющие минимизировать ложные оповещения тревожной сигнализации

Ресторанная сеть Panda (около 2000 точек) многие годы страдала от несовершенства системы тревожной сигнализации. Слишком часто поступали ложные сигналы. Менеджеров будили по ночам. Те, в свою очередь, немедленно связывались с полицией. Прибывшие наряды ничего криминального не обнаруживали. В одном только 2007 году корпорация заплатила почти полмиллиона долларов штрафов за сбои в системе.

Когда в 2008 году дипломированный специалист по безопасности Лил Форкум занял должность исполнительного директора Panda по вопросам охраны имущества, то первым делом решил установить новую, более совершенную систему сигнализации. Он выбрал фирму Interface (интегратор решений и информационных технологий), предложившую технологию, сочетающую в одном программном решении сигнализацию и видеонаблюдение. С установкой новой системы число ложных сигналов уменьшилось в пять раз. Полиция стала охотнее выезжать по сигналу тревоги, время прибытия на место потенциального происшествия сократилось с 30 до 5 минут. Уменьшилось и число реальных инцидентов благодаря добавленной функции верификации, исключающей использование скомпрометированных кодов для входа в ресторанное помещение при включенной сигнализации.

Как работает технология Interface? Система одновременно с тревожным сигналом автоматически передает на монитор дежурного охранника видео в реальном времени с того самого места, откуда пришел сигнал.

Технология предусматривает также установку в нужных местах динамиков и микрофонов, с помощью которых охранник располагает возможностью аудио коммуникации с рестораном. Данная функция оправдывает себя, прежде всего, в районах высокого криминального риска, так как позволяет на расстоянии вести переговоры с чересчур агрессивным посетителем (когда ресторан открыт) или с потенциальным преступником, освобождая персонал от необходимости улаживать вопрос.

Интерактивная видео и аудио система требует от работников ресторанной сети определенной подготовки, которую регулярно проводят с ними представители фирмы поставщика.

В ходе продолжения и углубления партнерства между Panda и Interface возможности видеонаблюдения интегрируются с системой электронного контроля за действиями кассиров, фиксирующей отклонения от установленных параметров работы. Любая подозрительная трансакция анализируется, в том числе, и с помощью архивной видеозаписи.

(по страницам журнала Security Magazine)

Огнестрельное оружие охранника. Плюсы и минусы

Владельцы кинотеатра Cinemark в городе Аврора (штат Колорадо) были оправданы по суду после того, как в 2012 году вооруженный молодчик расстрелял зрителей (12 убитых и более 70 раненых). Жюри сочло необоснованным обвинение администрации кинотеатра в том, что она была обязана обеспечить вооруженную охрану на премьере фильма.

А действительно, в каких случаях наличие у охранника огнестрельного оружия оправдано? Дебаты на эту тему ведутся в американской прессе уже несколько лет. Одни уверены, что само присутствие вооруженной охраны внушает чувство безопасности и отпугивает потенциальных террористов. Другие же полагают, что это только способствует нагнетанию опасной ситуации.

Тори Броунярд в своей статье на сайте журнала Security Management (ноябрьский выпуск за 2016 г.) рассматривает этот вопрос с точки судебных и страховых случаев. Он напоминает, что в США немногим меньше миллиона частных охранников (для сравнения: в стране 650 000 полицейских), и их число растет год от году в среднем на 5%.

В некоторых отраслях, например, в больницах, традиционно заботящихся о надежной безопасности, наличие вооруженных охранников вполне оправдано. Их численность в этой сфере возросла вдвое за последние четыре года. В 52% медицинских учреждений США охранники вооружены пистолетами, еще в 47% - электрошокерами.

Большинство людей приветствуют наличие огнестрельного оружия у охраны, особенно в местах повышенного риска, например, в банках.

Однако, пишет далее автор, пистолеты отнюдь не гарантия от опасности во многих других случаях. Более того, наличие дополнительного огнестрельного оружия может только увеличить число жертв. Огромна разница между охранником, использующим баллончик со слезоточивым газом, и охранником, открывающим стрельбу на поражение.

Если кто-то пострадал от применения охранником пистолета, то неизбежен судебный процесс. Охранному предприятию, помимо расследования полицией факта убийства

или ранения, грозит иск от страховых компаний. В очень редких случаях американский суд признает использование огнестрельного оружия обоснованным. Обычно такие инциденты характеризуются как превышение уровня необходимой защиты.

Такое решение на руку страховщикам, иски которых могут разорить небольшую охранную фирму. Важно иметь в виду, что для частной охранной деятельности рынок страхования весьма ограничен. Наем вооруженных охранников сужает его еще больше. На практике это означает, что такие компании будут платить много больше (по страхованию собственного персонала и страховым искам), чем их коллеги, обходящиеся без огнестрельного оружия. И это необходимо иметь в виду при заключении контрактов с клиентами.

В тех случаях, когда клиент настаивает на использовании вооруженных охранников, следует предпринять меры, которые бы минимизировали риски. Прежде всего, все охранники должны пройти строгую бэкграундную проверку на предмет того, не фигурируют ли они в неких «черных списках». Это в дополнение к обычной проверке на криминал. Эксперты советуют вооружать только тех охранников, которые в прошлом служили в армии или правоохранительных органах. Служба в полиции предполагает длительную и фундаментальную подготовку, умение разрядить конфликтную ситуацию без применения оружия.

Универсального ответа на вопрос, нужен ли пистолет охраннику, не существует. Принимая во внимание финансовые последствия, нужно принимать решение в каждом конкретном случае.

Затраты на кибербезопасность растут, но насколько они достаточны?

На этот вопрос отвечают эксперты в публикации журнала Chief Information Officer.

Затраты бизнеса на кибербезопасность растут скачкообразно по всему миру. Только в США за период времени 2015 – 2020, как полагают авторы доклада на сайте http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3, они составят 655 миллиардов долларов. Общемировые инвестиции в эту отрасль исчисляются триллионами долларов.

Корпорация IBM оценила свои потери от утечек и прочих кибер угроз в 2015 году в сумму 4 миллиона долларов. Статистика ущерба от киберпреступности и халатности, казалось бы, подсказывает необходимость наращивать усилия, соответственно и расходы, на повышение уровня информационной защиты. Но некоторые эксперты отмечают, что стоимость новых технологий безопасности может превышать реальный ущерб. Причем, значительно, если действовать строго в рамках рекомендаций компаний, производящих и продающих такие технологии.

С другой стороны, директор по информационной безопасности корпорации INTRALOT Кристос Димитриадис уверен: «Чем дольше вы затягиваете с инвестициями в кибербезопасность, тем дороже она вам обойдется в будущем». Он отмечает, что комплексное приобретение систем информационной защиты намного затратнее, чем постепенное обновление отдельный компонентов.

Конечно, ни одна организация не имеет бездонный бюджет на эти цели (быть может, за исключением Bank of America). Бизнесмены вынуждены мириться с отсутствием конкретных цифр, свидетельствующих о финансовой эффективности инвестиций в технологии безопасности (ROI – возврат вложенных средств). На уровне первых лиц, совета директоров идут острые дискуссии на эту тему. И очень часто на долю айтишников достаются не те деньги, на которые они рассчитывают, но существенно меньшие. Менеджеры по информации, безопасности, информационным технологиям, как правило, ясно представляют себе, что необходимо для надежной защиты корпоративных данных, но чаще всего вынуждены довольствоваться тем, что им выделяют.

Технологии кибербезопасности непрерывно усложняются. Поначалу они предназначались исключительно для охраны информации. Сегодня риски значительно серьезнее, они включают такое понятие как «работоспособность» бизнеса, которой угрожают атаки DDoS, могущие выводить из строя системы управления и контроля теми или иными операциями. Атаки хакеров год от года становятся все более изощренными и опасными, что вынуждает информационщиков и айтишников признавать: каким бы бюджет кибербезопасности ни был, 100% гарантированную защиту обеспечить невозможно.

Киберугрозы не только усложняются, но становятся и более динамичными, все быстрее обновляются, говорит директор по программным продуктам безопасности компании Radware, Бен Дежардин. Бизнесу сложно поспевать, отвечая адекватно на каждую новую киберугрозу. Поэтому все чаще приходится обращаться к помощи внешних специалистов. Конечно, аутсорсинг облегчает повседневную работу службы IT, но, с другой стороны, предполагает передачу функции защиты (частично или полностью) в чужие руки. А, следовательно, подчеркивает эксперт, в целом затрудняет управление и контроль системами безопасности.

Сегодня кибербезопасность представляет собой поле борьбы за соответствующие бюджетные ассигнования, за соблюдение правильного баланса между ценой технологий и их реальной эффективностью, за формирование достаточно гибкой финансовой политики в этом вопросе, позволяющей своевременно реагировать на происходящие в кибер пространстве изменения.

Флэш-моб как метод воровства в магазинах

В последнее время головной болью для розничной торговли в США стал флэш-моб. Речь не о невинных развлечениях молодежи, а о самых настоящих ограблениях, когда группа людей собирается как бы случайно у входа в магазин (хотя и случайность порой играет определенную роль), надвинув лоб бейсболки, врывается в торговый зал, хватает все подряд (или заранее намеченные вещи) и быстро исчезает. Все действие длится буквально секунды. Охранник, если таковой имеется, часто не успевает сообразить, что произошло, а полиция прибывает слишком поздно.

Из статистики последних месяцев. Таким способом был ограблен салон Apple в городе Нейтик (штат Массачусетс) – украдено аппаратов на 13 тысяч долларов. Магазин в Бостоне в результате флэш-моба понес убыток в 14 тысяч долларов. Список таких

деяний достаточно большой.

Такая тактика ограблений практикуется в США уже последние пару лет, но фокусировать на ней внимание пресса начала совсем недавно.

Отличительная черта последних месяцев – хорошая подготовка и организация. Налетчики используют для маскировки шерстяные головные уборы с прорезями для глаз и прочие маски. Более того, приносят с собой устройства, вырубающие на время сотовую связь.

Это уже не спонтанные действия, подчеркивает Эрни Дейл, пресс-секретарь Checkpoint Systems в интервью журналу Chief Security Officer, October 26, 2016. Их надо изучать и разрабатывать защитные меры.

Замечено, что флэш-мобы обходят стороной крупные торговые центры, где надежная охрана, много видеокамер, где собраться в группы незаметно для охранников практически невозможно. В этом смысле можно считать более безопасными магазины с большим потоком покупателей. «Никому не придет в голову залезать в переполненный автобус, чтобы через мгновения выйти в другую дверь», говорит Дейл.

По его мнению, решающую роль в предотвращении подобных преступлений имеет организация качественного контроля у входа в магазин. Кроме того, важно наладить хороший мониторинг покупателей в самом магазине, как с помощью видеокамер, так и посредством личного наблюдения и контакта продавцов с клиентами. В конечном счете, следует иметь заранее разработанный план предотвращения и реагирования.

Статистика воровства в розничной торговле показывает рост преступлений в период праздников. По данным американских экспертов, в 2016 году воровством занимался один из каждой тысячи посетителей. А в праздничные дни – один из 800.

В праздники самыми популярными объектами воровства являются одежда, детские игрушки, электроника.

Говоря о хищениях не надо забывать и о злоупотреблениях среди персонала, замечает Дейл.

В среднем по миру воровство в магазинах ежегодно увеличивается на 3 – 7 процентов в среднем. Причем растет оно быстрее там, где экономика переживает кризис.

Защита от мошенников в эпоху социальных медиа

Факт из реальной жизни. Бухгалтер американской компании получает по электронной почте указание от начальника, находящегося в отпуске, провести до конца дня валютный трансфер на один счет в китайском банке в рамках ведущихся переговоров о слиянии. В письме рекомендуется связаться с юристом компании, который также получил аналогичное указание. Обычный запрос, объясняла позднее бухгалтер, - из тех, которые она выполняла сотни раз. Все было сделано и в этом случае. Но уже на следующий день из телефонного разговора с начальником выяснилось, что последний никаких подобных поручений не давал.

Проведенное ФБР расследование показало, что сработала хитроумная мошенническая схема благодаря сведениям, очевидно собранным преступниками в социальных сетях. Именно там злоумышленники ищут и находят информацию, позволяющую им рассчитывать на успех. И это серьезная проблема для компаний, чьи руководители, менеджмент чрезмерно увлекаются социальными сетями, теряя бдительность и элементарную осторожность.

То же самое относится и к массовому распространению т.н. «интернета вещей». Исследовательская организация Gartrner полагает, что количество девайсов «интернета вещей», оцениваемое сегодня цифрой 6.4 миллиарда, к 2020 году возрастет до 20 миллиардов.

Согласно данным ФБР, с конца 2013 года более семи тысяч американских компаний были одурачены по схожим схемам. Чаще всего жертвами становятся сравнительно небольшие по размеру компании, в среднем теряющие от такого мошенничества порядка 130 тысяч долларов.

Подобным преступным промыслом занимаются не хулиганы подростки, лежа на диване. Это, как правило, высококвалифицированные преступники, объединенные в группы. Они днем и ночью отслеживают социальные сети и веб-сайты. Мониторинг популярных сетей, таких как Facebook и Twitter, а также данных с персональных, домашних девайсов позволяет выуживать информацию о том, в какое время дня вы находитесь вне дома, когда и где планируете отпуск, когда, где и с какими друзьями проводите свободное время…Преступники могут, например, выяснить в какое время главный бухгалтер занимается в тренажерном зале, а, следовательно, отрезан от дел и служебной переписки.

Что надо делать, чтобы минимизировать риски?

Грег Белл, руководитель американского отделения службы кибербезопасности транснациональной консалтинговой корпорации KPMG, рекомендует:

 Обеспечить персоналу компании, особенно менеджменту среднего и высшего звена, тренинги по поведению в социальных сетях, проводить их регулярно, с учетом меняющегося интернет ландшафта.

 Обеспечить работникам свободный доступ к инструментам безопасности, к примеру, к возможности составлять и часто менять сложные пароли.

 Установить жесткий контроль за финансовыми операциями, уделяя особое внимание поручениям на трансферы.

 В корпоративных сетях установить систему фильтрации e-mail трафика, реагирующую и сигнализирующую о письмах, похожих, но все же отличающихся от стандартной служебной переписки.

 Если возможно, взять под наблюдение все интернет домены, имеющие сходство с доменом компании.

 Моделировать потенциальные угрозы и риски.

Инсайдерские риски в сфере ЖКХ

Онлайновое издание Chief Security Officer (September 1, 2016) опубликовало статью по вопросу об инсайдерских рисках в сфере энергетики и ЖКХ.

Автор публикации Брайан Гаррел обращает внимание на тяжелые последствия как хакерских атак, так и физического несанкционированного проникновения на охраняемые объекты. Важно понимать, что внешние злоумышленники для достижения своих целей, а это обычно - вывод из строя оборудования, создание условий для экологической и гуманитарной катастрофы, нуждаются в изучении особенностей технологии производства. Для этого они часто прибегают к тактике наблюдения, пробным атакам, требующим немало времени. Но гораздо проще получить информацию изнутри, от сотрудников организации.

Согласно данным правоохранительных органов США, неоднократно фиксировались попытки преступников завербовать инсайдера. Им может быть не только действующий работник, но и бывший сотрудник самой компании – объекта нападения, либо партнерской организации, вообще любой человек, имевший когда-то доступ к технологиям или конфиденциальной информации.

Поскольку энергетика и сфера ЖКХ традиционно являются критически важной инфраструктурой в любой стране, там, как правило, действуют достаточно мощные системы безопасности, относящиеся как к физической охране, так и к защите информации. Проблема в том, подчеркивает автор статьи, что эти системы изначально ориентированы на внешние угрозы, в то время как самые серьезные риски могут проявиться внутри. Не секрет, что собственные работники, постоянные и временные, поставщики и прочие партнеры имеют зачастую неограниченный доступ к тому, что следовало бы строго охранять.

Спецслужбы США признают, что персонал на объектах важной инфраструктуры зачастую не имеет ясного представления о реальных угрозах потенциального инсайдерства. Поэтому первостепенное значение приобретают учебные программы, которые бы включали занятия по распознаванию признаков внутренних рисков и угроз, по соблюдению инструкций и политик безопасности, по способам информирования и реагирования на потенциальные инциденты. В проведение тренингов должны активно включаться служба безопасности компании, отдел кадров, служба информационных технологий.

Автор статьи называет наиболее важные, по его мнению, направления работы по выявлению и минимизации внутренних угроз:

Формирование в компании соответствующей культуры отношения к внутренним рискам

В частности, корпоративной службе безопасности следует проводить регулярные брифинги с разъяснением инструкций и процедур, которые необходимо неукоснительно всем соблюдать.

Формирование понятной каждому системы мер по информированию руководства о

подозрительном поведении

Это очень важный компонент предотвращения инцидента безопасности. СБ обязано наладить контроль за поведением сотрудников и мотивировать «стукачество» в лучшем смысле этого слова.

Налаживание и поддержка тесного взаимодействия с региональными правоохранительными органами

Работники, представляющие потенциальную опасность для организации, могут иметь связи с преступниками, на которых в полиции имеется досье.

Постоянный анализ рисков

Необходимо прогнозировать и анализировать возможные инциденты, связанные с инсайдерами, и их последствия для организации.

Йельский Университет модернизирует систему СКУД

Когда в 2013 году аноним по телефону пригрозил устроить бойню, служба безопасности Йельского университета немедленно заблокировала все входы и двери центрального кампуса в Нью Хэвене, штат Коннектикут. Каждому из находившихся там было велено «окопаться и не высовываться».

Расследование, проведенное ФБР, не обнаружило террориста. Но сам инцидент, по словам руководителя университетской СБ Роннелла Хиггинса, предоставил хорошую возможность проверить на деле надежность систем охраны. «Мы взглянули на ситуацию с точки зрения того, что надо еще сделать для повышения эффективности систем безопасности», сказал он в интервью журналу Security Management (декабрьский номер за 2016 г.). В университете учатся 11 тысяч студентов. Административно-преподавательский состав превышает три тысячи.

Самая сложная для СБ задача, продолжает Хиггинс, это обеспечить правильный баланс между необходимым уровнем безопасности и открытым, дружелюбным климатом. «Мы не хотим превращать ВУЗ в подобие крепости».

После упомянутого инцидента с анонимной угрозой университет предпринял шаги по модернизации СКУД. Во-первых, был создан единый центр мониторинга и управления. Во-вторых, приняты меры по ужесточению контроля за доступом на территорию кампуса и в помещения как студентов и преподавателей, так и гостей, посетителей. В-третьих, усовершенствованы процедуры блокирования и изоляции зданий в случае форс-мажора.

Чтобы понять, какие именно технологии СКУД следует внедрить, университет нанял

внешнего консультанта, с участием которого были проведены переговоры с рядом крупных поставщиков. Решили остановиться на продукте Symmetry SR Solution компании AMAG. В 2014 году началась работа по замене старых решений, и к настоящему времени две трети университетских зданий уже оснащены более совершенной технологией.

Выбор не случаен. Компания AMAG предложила сохранить имеющее компьютерное оборудование. Более того, она использовала существующую кабельную инфраструктуру для поддержки считывателей электронных пропусков во всех зданиях университета. Это стало решающим аргументом в пользу AMAG. Некоторые здания построены более 200 лет назад, и полная замена всех сетей потребовала бы дополнительно миллионы долларов.

Экономичным и эффективным шагом стало образование единого центра управления. Реализация проекта позволила интегрировать системы видеонаблюдения и тревожной сигнализации. Теперь с помощью новой технологии операторы получили возможность блокировать отдельные здания и помещения по сигналу тревоги.

Введение новой программы в систему электронных пропусков проходит фактически незаметно для пользователей. У них на руках те же карты, что и раньше. Коды чипов меняются дистанционно электронным способом. Правда, некоторые обладатели обнаружили, что их карты более не действуют. Команда специалистов в таких случаях вмешивалась и обеспечивала совместимость пропусков с новой технологией.

Первые два года осуществления проекта в университете постоянно работал инженер AMAG. Это помогало быстро решать возникающие технические и технологические проблемы.

Полностью проект будет завершен к концу 2017 года.

Как защитить коммерческий сайт от мошенников, хакеров и ворующих торговые марки

В наши дни нетрудно создать веб-сайт для коммерческих целей. Намного сложнее его защитить от разного рода злоумышленников, которые могут разрушить ваш бизнес.

Дженнифер Шифф, автор статьи в журнале Chief Information Officer, предлагает свои рекомендации по защите.

Регистрируйте торговую марку и логотип

Это первый важный шаг защиты от потенциальных нарушителей коммерческого права. Основатель компании Organic Aromas Джон Джойнс рассказывает о попытке китайского коммерсанта скопировать не только продукцию, но и рекламу, и маркетинговую информацию его фирмы. Свою противоправную деятельность китаец прекратил после получения официального запрета со ссылкой на законы, защищающие зарегистрированные торговые марки и интеллектуальную

собственность.

Используйте проверенные и надежные платформы для электронной торговли

Такие платформы обладают функцией мониторинга всех размещенных на них торговых сайтов и позволяют вовремя обнаружить и предотвратить неправомерные, потенциально угрожающие безопасности действия.

Используйте технологию SSL (Secure Sockets Layer)

Это стандартная технология безопасности, обеспечивающая шифрованную связь между веб-сервером и браузером. Она особенно необходима в таких операциях как электронные расчеты (трансакции), надежно защищает важную финансовую и персональную информацию от потенциальных преступников. Между тем, отмечают эксперты, очень многие коммерческие веб-сайты игнорируют данную технологию

Обеспечьте стандарт безопасности PCI DSS

PCI DSS - стандарт безопасности данных индустрии платежных карт, объединивший в себе требования международных платежных систем к информационной безопасности.

Регулярно обновляйте сайт

Хакеры любят срывать низко висящие плоды. Они ищут объекты с дырявой, устаревшей защитой. Своевременное обновление технологии информационной защиты - важнейший шаг в обеспечении безопасности интернет бизнеса.

Применяйте сложные пароли и коды

Один из методов хакерства – автоматический подбор комбинаций букв и цифр для взлома корпоративной сети. Специалисты советуют использовать длинные и случайно набранные комбинации с прописными и обычными знаками. Менять пароли надо как можно чаще, но не реже раза в полугодие.

Умейте различить признаки мошенничества

Необходимо обращать пристальное внимание на адреса и имена авторов электронных посланий, доменные имена, проверять клиентскую историю (злоумышленники часто прикидываются клиентами), а также быть в курсе методов и способов мошенничества,

характерных для страны или района вашего пребывания и работы.

Как обезопасить компанию с дистанционно работающими сотрудниками

С внедрением мобильных устройств в бизнес процессы, с набирающей популярность удаленной от офиса (дистанционной) работой, встал вопрос, как защитить корпоративные данные от утечек и хищений.

Информационно-консалтинговая компания Wombat Security Technologies предлагает свои рекомендации на этот счет.

Ограничить пользование WiFI открытого доступа

Такие сети недостаточно защищены для передачи с их помощью важной служебной информации (клиентские данные, номера кредитных карт, и т.п.). Командированным работникам рекомендуется использовать встроенные в их мобильные устройство функции интернета.

Обеспечить надлежащую защиту домашней сети

Минимум что надо сделать – «запаролить» сеть и ввести шифрование.

Установить VPN на всех мобильных устройствах, используемых для работы

Большинство организаций с дистанционными сотрудниками использует VPN (обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети), но это касается скорее офисных, а не персональных устройств. Эксперты советуют обязательно распространить эту технологию и на личные средства коммуникации, если они используются для работы.

Заменить слабые пароли на более сложные

Работающие дома сотрудники часто подключают корпоративные девайсы к домашним (WiFI, беспроводной принтер, и т.п.). Необходимо добиваться, чтобы дистанционные работники устанавливали на все виды домашних и офисных устройств (особенно на роутеры) достаточно сложные пароли.

Не смешивать корпоративные и личные данные

Пресса часто пишет об утечках служебной информации через персональные девайсы, предназначенные для личных целей. Такую практику необходимо запретить.

Не злоупотреблять социальными сетями

Работающие дома нередко утрачивают чувство предосторожности, заходя в социальные сети, случается, выбалтывают детали своей работы, что чревато негативными последствиями. То же самое касается и командированных лиц.

Вовремя обновлять программные продукты

Киберпреступники постоянно ищут сетевые уязвимости, которые характерны для устаревших технологий. Поэтому важно своевременно обновлять Adobe Flash, Acrobat Reader, другие приложения и решения.

Не подпускать к служебной информации посторонних

К дистанционному работнику домой приходят соседи, родственники, гости. В этом случае необходимо закрывать все устройства, предназначенные для работы и хранить их в недоступных дл посторонних местах. Важно также не забывать, что служебные переговоры по телефону, скайпу могут быть подслушаны теми, для кого информация не предназначается, включая близких родственников.

Не забывать о надлежащей физической защите

Уже говорилось, что все служебные девайсы и материалы должны храниться в недоступном для других месте. Тем, кто в пути, рекомендуется не забывать устройства в машине, не оставлять без надзора в кафе и других местах общего пользования.

Создание условий для карьерного роста внутри компании

Постоянный автор журнала Security Magazine Джерри Бреннан опубликовал заметку о перспективах карьерного роста специалистов по корпоративной безопасности в рамках одной организации.

Опираясь на собственный опыт исследования многих компаний, он указывает на типичный сценарий: увольняющийся охранник или офицер по безопасности чаще всего уверен, что его место займет коллега по работе, в то время как в действительности организация не занимается выращиванием собственных талантов, а потому вынуждена обращаться на рынок труда.

Бреннан убежден в целесообразности разработки и реализации собственной

программы подготовки специалистов с прицелом на замещение уходящих по тем или иным причинам сотрудников и предоставление наиболее способным сотрудникам условий для служебного продвижения. В этом контексте автор заметки предлагает руководителям корпоративной службы безопасности следующие шаги:

 Проанализировать уровень профессиональной квалификации и личностных качеств членов команды, насколько они отвечают текущим требованиям и каким должны быть в обозримом будущем.

 Предоставить сотрудникам СБ возможность профессионального общения с руководителями других управлений в компании, чтобы наглядно ознакомиться и лучше понимать бизнес процессы.

 Не упускать возможности для участия сотрудников в мультифункциональных проектах организации, способствующих их интеграции в культуру компании, осознанию себя как неразрывной части организации.

 Использовать корпоративные тренинги, проводимые отделом кадров и другими управлениями организации, для участия в них сотрудников СБ.

 Использовать по возможности и внешние учебные программы и курсы. Нетрудно найти (в США) общедоступные тренинги по развитию профессиональных качеств. На этих курсах сотрудники смогут проверить свои компетенции, выявить слабые места и возможности для повышения квалификации.

 Не игнорировать тех, кто работает в заграничных филиалах. Регулярно приглашайте их на учебу в штаб-квартире компании. Этим вы демонстрируете заинтересованность в их карьерном и профессиональном росте, даете понять, что им нет необходимости искать лучших возможностей в других организациях.

The Guide to Online Due Diligence Investigations

By Cynthia Hetherington, CFE
BRB Publication. Available from ASIS, № 2247
336 pages

Многие частные сыщики, расследователи выполняют свою работу в интернете рутинным путем: одни и те же инструменты, одни и те же сайты, одни и те же методы.

Рецензируемое издание предлагает огромный выбор инструментов и практик, помогая специалисту выйти на новые рубежи своей профессии.

В вопросах как бэкграундной проверки при приеме на работу, так и изучения потенциального партнера, книга предоставляет возможность выбирать такие инструменты и методы, которые обеспечивают наилучший результат.

Читатель много интересного и полезного узнает о малоизвестных или совсем неизвестных ему/ей источниках информации.

Книга содержит примеры, образцы отчетов (для клиента) и контрактов, обширный перечень источников в социальных сетях.

Монография также предлагает конкретные рекомендации, основанные на практическом опыте автора.

Издание заслуживает постоянного места на рабочем столе частного сыщика и расследователя. Оно не менее полезно и для работников государственных органов правопорядка.