Охрана предприятия

№4 (44), 2015

Оглавление

Как минимизировать проблемы, обусловленные человеческим фактором

Снаряжение охранника

Книжное обозрение

Integrated Electronic Security: A Layered Approach
2/9/2015 by Martin Grigg; Reviewed by Terry L. Wettig, CPP

Investigating Internet Crimes
6/1/2015 by Todd Shipley and Art Bowker; Reviewed by Ben Rothke

Исследования

Угрозы знают лучше, но по-прежнему ведут себя безответственно

В период летних отпусков хакеры нацелились на отели и авиакомпании

Финансовые институты худо-бедно научились выстраивать защиту против киберпреступников, и последние ищут новые, более простые и доступные пути наживы. В числе лакомых объектов – отели и авиакомпании, особенно в разгар массовых отпусков. Еще весной хакеры успешно взломали базы данных Lufthansa и Airways, популярного агентства путешествий Starwood (управляющей компании, предоставляющей в различных странах мира гостиничные услуги под брендами Sheraton). Об этом сообщает веб-портал cio.com.

Автор размещенной там статьи Джен Миллер отмечает, что множество туристических фирм и транспортных контор слабо защищены от киберпреступников. Среди них такие известные авиакомпании как American Airlines, такие популярные сетевые отели как Marriot. Исключение составляют Booking.com и авиакомпания Delta, по оценке компании Agari, специализирующейся на вопросах безопасности электронной почты.

Методы кражи персональных данных примерно одни и те же. Преступники от имени реальных и вымышленных организаций рассылают фишинговые письма, а также поддельные инвойсы, ваучеры, авиабилеты, чтобы любыми способами проникнуть и заразить персональные компьютеры. Когда получатели фальшивок кликают на предлагаемые ссылки, то попадают на сайты, которые выглядят солидно, как подлинные ресурсы гостиничного и транспортного бизнеса.

Обманутый пользователь, что еще хуже, начинает отвечать на обычные, стандартные вопросы и невольно выдает злоумышленникам конфиденциальную информацию о себе.

Некоторые липовые сайты продают несуществующие номера в гостиницах, либо

существующие, но без права заниматься этим делом. Они демонстрируют привлекательные фотографии номеров, которые уже давно заняты или забронированы, либо не существующих в природе.

Получив обманным путем персональные данные кредитных карт, крадут деньги, либо продают информацию другим мошенникам. Овладев логином и паролем, преступники тестируют их через разные сайты, выясняя, где еще жертва хакерства пользуется ими для оплаты услуг, товаров.

Компаниям стоит немало денег компенсировать своим клиентам потерянные по вине мошенников средства. Еще больший урон наносится их репутации. Обманувшись хотя бы раз, люди склонны с подозрением, недоверием относиться к реальным предложениям реальных агентств.

Какими компетенциями должен сегодня обладать руководитель корпоративной службы безопасности

Тед Шлейн (Ted Schlein), Генеральный Партнер компании Kleiner Perkings Caufield & Byers, пишет в журнале «Forbes»: «Сегодня лидеры бизнеса наконец-то начинают осознавать значение охраны предприятия, понимают, насколько трудно, но крайне необходимо, обеспечивать защиту компании, прежде всего, клиентской информации от атак злоумышленников».

Данная цитата воспроизведена в онлайновом издании Security Magazine, в статье редактора Даяны Ритчи (5 июня 2015). Здесь же приводится и другое высказывание Шлейна: «Я постоянно говорю, что руководитель корпоративной безопасности является краеугольным камнем успешного бизнеса, и он должен обладать компетенциями, которые редко встречаются в одном лице».

Другой эксперт, Джерри Бреннан (Security Management Resources Group), недавно завершил исследование деловых качеств идеального руководителя СБ на основе опроса первых лиц в 39 компаниях (всего было опрошено 67 бизнесменов). В результате был сформирован список компетенций, выстроенный по частоте упоминаний:

- высокие моральные, этические качества;
- деловая хватка;
- честность;
- умение контактировать с топ-менеджментом;
- стратегическое видение;
- хороший письменный стиль;
- фокус на клиентуру;
- умение принимать решения;
- способность ориентироваться в условиях неопределенности;
- организаторский талант;
- умение формировать эффективную команду;

- понимание задач и целей;
- умение презентовать отчеты;
- смелость в принятии управленческих решений;
- умение мотивировать подчиненных;
- собранность (хладнокровие);
- коммуникабельность (общительность);
- умение выслушивать других;
- правильная политическая ориентация;
- прочие качества...

Авторы исследования не удивлены, что две из первых трех позиций относятся к моральным аспектам. Корпоративная безопасность – это та область бизнеса, где честность, порядочность, нравственность особенно важны и высоко ценимы.

Второй момент, обращающий на себя внимание экспертов, - огромное значение коммуникабельности, правильного выстраивания взаимоотношений на всех уровнях: с начальством, коллегами, подчиненными. Именно от этого личностного качества зачастую зависит карьера.

Третий важный аспект – понимание особенностей и, главное, перспектив бизнеса компании, распознавание новых тенденций в быстро меняющемся мире. Необходимо думать на перспективу, что будет с бизнесом и компанией через год, два, три, четыре, пять лет, какие новые риски и угрозы вырастают на горизонте, как должна перестраиваться работа службы безопасности.

(окончание в следующем выпуске журнала)

Карьерный успех через самооценку

Четко понимать свои возможности, компетенции и интересы, соответственно ставить ясные цели и планировать ближайшие шаги, стремиться к повышению квалификации до необходимых уровней – необходимые условия для успешной карьеры в области корпоративной безопасности, пишут постоянные авторы журнала Security Magazine Дж. Бреннан и Л. Маттис (впрочем, эти сентенции можно отнести к любой сфере деятельности – ред.).

Авторы публикации в июльском номере журнала фокусируют внимание на методологии самооценки и самопроверки, особенно востребованной для тех, кто ищет руководящую работу в сфере корпоративной безопасности. Выделяют следующие личные качества и компетенции, требующие обстоятельного самоанализа:

Интуиция и психологическая проницательность (эмпатия). Способность разбираться в характерах и способностях других людей помогает формированию атмосферы доверия в коллективе, что является важным условием стимулирования эффективного, плодотворного труда. С другой стороны, слишком мягкое, излишне доверчивое отношение к подчиненным чревато возникновением проблем.

Ориентация на результаты и решительность. Способность мотивировать подчиненных на интенсивный труд, смотреть на трудовые процессы через призму ожидаемых результатов, ориентация коллектива на достижение этих целей. Насколько комфортно

вы чувствуете себя в вопросах, которые недостаточно глубоко знаете? Как вы ведет сбор информации для принятия решений, в каком объеме и качестве информации испытываете нужду? Легко ли поддаетесь убеждению со стороны? Хватает ли у вас решимости принимать сложные решения?

Способность к осмыслению (reasoning). Нравится ли вам делать рутинную работу? Достаточно ли вы креативны? Считаете ли вы свое мнение единственно верным в черно-белой ситуации? Вы по характеру оптимист или скорее пессимист?

Дисциплинированность и организованность. Умение планировать, структурировать и анализировать идеи; следовать установленным правилам, указаниям, логике вещей; способность и желание совершенствовать инструкции, политики и процессы. Здесь важно понять, уяснить свою роль в организации, где собираетесь работать. Возможно, вам будет там комфортно работать, но в целом корпоративная культура будет чужда.

Взгляд на себя. Как вы реагируете, если вам отказывают в идеях и предложениях? Как относитесь к возникающим вызовам? Находите ли вы у себя энтузиазм и хорошее воображение?

Виды на будущее (что ждете для себя). Ваши личные цели и ожидания. Вы по характеру уступчивы или упрямы? Способны ли идти наперекор ходу вещей?

Если в процессе самоанализа вы обнаружите, что в одном-двух из перечисленных качеств слабоваты, это не означает крах надежд. Понимание своих сильных и слабых сторон – большое преимущество. Еще до презентации своего резюме можете сделать вывод, годитесь на приглянувшееся вам место или нет. В последнем случае не лучше ли поискать другую, более подходящую работу и организацию.

Углубленная самооценка имеет и другой важный аспект. Вам уже не составит труда четко отвечать на вопросы, которые любят задавать соискателю на собеседовании кадровики и потенциальные руководители относительно стиля, интересов, предпочтений и т.п.

Переходный этап для технологий банковской безопасности

В то время как налеты на банки становятся все реже, на первое место среди угроз вышли мошеннические операции с использованием интернет-технологий (скимминг, кража данных персональной идентификации, и т.п.). Соответственно трансформируются и технологии защиты от банковских преступлений. К примеру, компания Diebolt, с момента своего возникновения в 1859 продолжительное время специализировалась на производстве металлических сейфов, обустройстве подвальных хранилищ, запорных устройств. К настоящему времени компания превратилась в поставщика исключительно программных продуктов, призванных защищать банкоматы и офисы банков от мошенников.

В статье Б.Залуда, постоянного автора онлайнового журнала Security Magazine (June, 2015), речь идет о некоторых технических и технологических тенденциях в сфере

банковской безопасности.

Привлеченные автором публикации эксперты отмечают, что центральное место в системе охраны банков играет видеонаблюдение. Здесь заметна тенденция к сокращению количества камер, установленных внутри и снаружи конкретного объекта, при одновременном усилении их разрешающей способности, более широкого угла обзора, внедрении средств архивации. Переход к видеокамерам высокого разрешения (от аналоговых к цифровым) совершается постепенно, так как большинство банков реализуют планы, рассчитанные на несколько лет. Новые технологии позволяют не только проводить расследование по следам совершенного преступления или попытки такового, но и экономить средства благодаря уменьшению числа установленных камер, подчеркивает Мэтт Фроуэрт, директор по финансовым услугам корпорации Tyco Integrated Security.

Предлагаемые на рынке инновации успешно заменяют традиционные дверные замки и ключи. Электронные системы СКУД позволяют устанавливать и контролировать временные и территориальные зоны для банковских служащих и клиентов. Соответственно совершенствуются средства идентификации. Эксперты предсказывают появление уже в самом ближайшем будущем и массовое распространение технологии голосовой идентификации по телефону.

Защита банкоматов – головная боль банкиров. Широкое внедрение анти-скиммингговых продуктов не отменяет необходимости при установке банкоматов учитывать и улучшать физические условия, например, освещенность помещения, и даже такие детали, как наличие густой растительности (деревьев и кустов) вокруг здания.

Особого внимания заслуживает тенденция к интеграции средств физической и информационной защиты. На эту тему в США регулярно проводятся научно-практические конференции и круглые столы. Подобное мероприятие прошло весной этого года в Университете Феникса (штат Аризона), который занимает лидирующее место среди американских вузов по онлайн-обучению. Комментирует Джон Ферранти, декан факультета физической и информационной защиты: «В дискуссиях приняли участие представители разных сегментов сферы безопасности. Основное внимание уделялось кибербезопасности. И это понятно. Вульгарный грабитель может поживиться в банке тысячами долларов, в то время как хакеры уводят миллионы баксов. Грабителя несложно вычислить и поймать. А шансов изобличить и обезвредить кибермошенников, специализирующихся на банках, очень сложно, зачастую просто невозможно», Ферранти отметил, что круглый стол продемонстрировал четкую тенденцию к интеграции технологий и взаимодействия профессионалов физической и информационной защиты. Он подчеркнул необходимость упреждающего подхода к вопросам банковской безопасности. По его мнению, спрос банкиров на руководящие кадры в сфере корпоративной безопасности будет в ближайшее время возрастать на 13% ежегодно.

Кадровый аутсорсинг в сфере

кибербезопасности

Сегодня, когда киберугрозы растут как снежный ком, рынок труда в сфере корпоративной безопасности испытывает острейший дефицит опытных руководителей. Согласно исследованиям солидных западных организаций (в их числе – Frost & Sullivan), примерно две трети всех крупных международных компаний страдают от нехватки высококвалифицированных специалистов в области информационной защиты. Число соответствующих вакансий в мире растет и, по некоторым экспертным прикидкам, достигнет через пять лет гигантской цифры в полтора миллиона.

В этих условиях компании все чаще прибегают к аутсорсингу, приглашая сильных специалистов на руководящие должности по временным контрактам. Эту тенденцию комментируют эксперты в статье Б. Виолино, размещенной на сайте csoonline.com.
Положительная сторона «аренды» специалистов заключается в том, что компании получают возможность выстраивать программы и планы информационной защиты, опираясь на квалификацию и опыт приглашаемых со стороны консультантов, отмечает Джереми Кинг, президент компании Benchmark Executive Search. Недостаток такого подхода проявляется в трудностях создания и управления всеобъемлющей программой кибербезопасности при отсутствии своего, штатного, постоянного специалиста, продолжает эксперт.

Макс Олах, президент компании MAFAZO Digital Solutions, выступает в качестве «виртуального» руководителя по вопросам информационной защиты сразу в нескольких организациях, как крупных, так и мелких. По его словам, он помогает клиентам формулировать «дорожные карты» кибербезопасности, управляет техническим персоналом, анализирует и докладывает первым лицам информацию об угрозах на понятном им языке, консультирует финансовых директоров. Оплата почасовая.

Для крупных компаний аренда специалистов – временная вынужденная мера. Для малых предприятий – обычная практика, так как пригласить в штат высококвалифицированного эксперта они не могут из-за финансовых ограничений.

Макс Олах считает данный аутсорсинг «выгодным для бизнеса». Приглашаемые извне профессионалы не только успешно решают сложные технические задачи, но и, как правило, умеют разговаривать на равных с топ-менеджментом, представляя доступную картину киберугроз и потенциальных последствий.

Андреа Хоу набиралась опыта в качестве специалиста по вопросам безопасности в таких корпорациях как Rockwell и Boeing. Сегодня она – «виртуальный» руководитель службы информационной защиты, обслуживающий небольшие частные компании. В чем конкретно заключается ее работа? В некоторых компаниях она помогает наладить работу штатному специалисту по кибербезопасности, который только что пришел на эту должность без достаточного практического опыта. В других организациях она временно замещает вакантную должность, пока не найден и не принят в штат постоянный профессионал. В частности, помогает в поиске подходящей кандидатуры.

Стоит ли идти компаниям по пути временной аренды? Как считают эксперты, ответ на вопрос зависит от разных конкретных обстоятельств. Например, от временных рамок

проекта кибербезопасности, от структуры организации, корпоративной культуры, финансовой составляющей...

Нет смысла обращаться к кадровому аутсорсингу, если компания не готова к инвестициям и серьезной перестройке в сфере информационной защиты, говорит Макс Олах. Иногда бизнесмены приглашают хорошего специалиста, рассчитывая на волшебные изменения, но при этом не собираясь вкладываться в развитие проекта. Кроме того, аутсорсинг неуместен, если предприниматели не готовы «делить» специалиста с другими организациями из-за боязни информационных утечек.

(по материалам веб-сайта scoonline.com)

Как добиться финансовой поддержки на развитие СБ

Постоянный автор журнала Chief Security Officer М. Сантарканжело указывает на разницу между понятиями «бюджет» (budget) и «финансирование» (funding). В первом случае речь идет о заранее спланированных расходах, во втором – об инвестициях на развитие, на решение возникающих проблем. Автор публикации предлагает ряд советов, что следует делать руководителю СБ, чтобы заручиться поддержкой кампании в вопросах финансирования.

Как ни странно, он рекомендует для начала обратиться за помощью к финансовому директору компании, так как последний имеет ясное представление о финансовых источниках и возможностях. Можно также посоветоваться с кем-нибудь из менеджеров, имеющих диплом МБА, интересующихся вопросами корпоративного финансирования. У коллег могут быть интересные соображения на этот счет, которые пригодятся в процессе подачи и защиты заявки.

Для подготовки убедительного документа необходимо объективно взвесить, какие приоритеты надо выделить, в чем больше всего нуждается СБ в данный момент и ближайшее время. Одновременно учитывайте приоритеты, стоящие перед всей компанией. В заявке важно увязать между собой и те, и другие. Такой подход существенно повышает шансы на успех.

Полезно сравнить, как обстоят дела у вас и у ваших партнеров, конкурентов (в соответствующих подразделениях). Собранная информация выявит тенденции в сфере безопасности (в данной отрасли экономики, бизнеса), высветит стоящие перед СБ общие проблемы, возможно, даже подскажет, к каким результатам ведет намеченный вами и требующий инвестиций проект.

В большинстве случаев запрашиваемые службой безопасности средства предназначены на приобретение новых охранных технологий. Никто не хочет отставать от прогресса. Тем более, если конкуренты уже обзавелись новинками. В этом случае целесообразно изучить, как новые системы работают у них, поразмышлять о пригодности для внедрения в своей компании. Но здесь надо проявлять здравый смысл. Инновации обычно стоят дорого, но далеко не всегда и не везде дают ожидаемый результат. Важен баланс между риском затрат и

прогнозируемой отдачей.

В заявке на выделение денег необходимо убедительно продемонстрировать, как вложенные средства усилят безопасность компании, в конечном счете, отразятся на доходах и прибылях. Зачастую трудно рассчитать в цифрах «оборачиваемость», конечную финансовую эффективность для компании вложений в безопасность. Но стремиться к этому необходимо.

Важен и язык заявки. Он не должен быть перегружен техническими терминами и понятиями. Помните, что те, кто принимает окончательное решение, не обязаны владеть специальными познаниями в технологиях безопасности. Им надо уяснить, каким образом предлагаемые инвестиции помогут решить ту или иную бизнес проблему, повысят эффективность работы, повлияют на добавленную стоимость. В этом смысле очень кстати может оказаться пример аналогичной «успешной истории» у партнеров или конкурентов.

Инсайдерские риски в аэропортах

Этой теме посвящена пространная статья Л. Чейпа в ежемесячном журнале Security Management, июньский выпуск 2015 года.

Международный аэропорт в городе Атланта (США) – один из самых загруженных в мире. Обслуживают аэропорт 63 000 людей. Сюда же включен персонал авиакомпаний, пользующихся аэропортом. Все они проходят предварительную бэкграундную проверку и получают пропуска в те или иные зоны и помещения.

Тем не менее, получили гласность серьезные нарушения правил безопасности, связанные с незаконным провозом оружия из Атланты в Нью-Йорк. В одном преступлении замешанным оказался служащий Delta Airlines, в другом – инспектор Федерального управления гражданской авиации США. Оба воспользовались пропуском на перемещение по аэропорту Атланты.

По мнению автора статьи, требования федеральных регуляторов США к охране и соблюдению безопасности в аэропортах «довольно либеральны». К примеру, только в двух американских аэропортах всех служащих заставляют ежедневно проходить контроль металлодетекторов при входе на территорию аэропорта наряду с простыми пассажирами.

До настоящего времени в большинстве аэропортов не принято проводить криминальную проверку служащих после того, как они приняты на работу. Проверка повторяется иногда перед переводом на новое место с повышением.

Сегодня Управление транспортной безопасности (в составе министерства транспорта США) готовит рекомендации, которые, в частности, включают создание базы отпечатков пальцев всех без исключения работающих в сфере авиаперевозок, а также регулярную (повторную) их бэкграундную проверку.

Основания для ужесточения правил безопасности налицо. Так, например, установлено,

что за последние два года в международном аэропорту Атланты было потеряно почти полторы тысячи служебных пропусков. Они немедленно дезактивируются, как только о потере докладывают. Но проблема в том, что такая информация нередко запаздывает.

При этом отмечается довольно равнодушное отношение администрации к исчезновению пропусков. Такие случаи не рассматриваются как серьезная угроза безопасности, поскольку при входе в «стерильную зону» («стерильной зоной» в аэропорту называется территория контролируемого доступа, которая начинается за первыми пунктами контроля и досмотра пассажиров и заканчивается у входа в самолет) помимо служебного пропуска необходимо предъявить фото ID, а для некоторых помещений набрать специальный код. Однако, возражают эксперты, даже плохой актер способен с помощью украденного пропуска и подделанного фото преодолеть охраняемый периметр.

При этом речь идет не только о штатных работниках аэропорта, но и о тех служащих, которые, находясь на территории аэропорта, обслуживают авиакомпании. У них даже есть свой профсоюз, насчитывающий (в США) 12 000 человек. Это те, кто готовит и доставляет на борт еду, водители, уборщики салонов, механики, слесари и т.д. Именно эта категория служащих, утверждают эксперты, заслуживает особо пристального внимания и более жестокого контроля, включая тщательный осмотр грузовиков и фургонов.

Проведенный среди них опрос показал следующие цифры:

- только 33% заявили, что у них на кухнях осуществляется жесткий контроль;
- 24% признали, что вход в их рабочие помещения фактически не охраняется и зайти может кто угодно;

Не лишним будет добавить, что во вспомогательных, обслуживающих авиакомпании организациях чрезвычайно высока текучесть рабочей силы – 44% в год.

Использование персональных данных при контроле доступа – риск для бизнеса

Об этом пишет Стив Рэган, обозреватель журнала Chief Security Magazine, ссылаясь на мнение экспертов по вопросам безопасности. Один из них, Скотт Уэбб, имел случай на собственном опыте убедиться, что использование персональной информации для доступа к закрытым ресурсам опасно.

Однажды ему понадобилось перекинуть деньги с одного счета на другой, но по каким-то причинам не мог воспользоваться инструментом онлайн банкинга, а потому решил обратиться в службу поддержки банка Delta Community Credit Union. Оператор для проверки попросил клиента назвать последние четыре цифры социальной страховки, домашнего адреса, телефона и номера банковского счета. Информацию по первым трем позициям в принципе можно отыскать в открытых источниках, а четвертая

позиция – самая важная и сугубо конфиденциальная – вполне может быть раскрыта путем т.н. «социального инжиниринга» (получения несанкционированного доступа к информации без применения технических средств, с использованием особенностей психологии человека). Позднее Уэббу опять пришлось позвонить в тот же банк, и вся процедура вновь повторилась. Оператор спросил последние цифры по тем же позициям, затем перенаправил клиента в соответствующий отдел банка, где пришлось отвечать на те же вопросы плюс называть еще номер дебитной карты.

По мнению ряда экспертов, проверочные вопросы, базирующиеся на фактах личной жизни, могут служить методом персональной идентификации при условии, что эти факты известны строго ограниченному кругу лиц, лучше всего, двоим, т.е. участникам телефонного диалога. Но когда одна и та же информация (к примеру, девичья фамилия матери, имя любимого школьного учителя, кличка домашнего животного,...) используется постоянно, то надежность этого способа деградирует. Чем больше людей овладевают конфиденциальной информацией, тем труднее держать ее в тайне от потенциальных злоумышленников.

Хотя банковские служащие уверяют, что чередуют, меняют проверочные вопросы каждые несколько дней, Уэббу ни разу не предложили иной набор вопросов.

В идеале, банки и другие финансовые организации должны исключить вопросы, ответы на которые можно найти в открытых источниках (номера телефонов, адреса и пр.), утверждает Роберт Хансен, вице-президент WhiteHat Security. Проверка должна строиться на информации, которую никак не могут знать посторонние. Например, вопрос может звучать следующим образом: «Три недели назад вы сняли со счета 300 долларов, каким банкоматом воспользовались?». Или: «Скажите, сколько вы заплатили со счета по ипотеке в прошлом месяце?».

Понятно, что потребители банковских услуг предпочитают пользоваться удобными, простыми и легкими способами доступа к своим счетам. Если комфорт и соображения безопасности вступают в противоречие, то их выбор – в пользу первого. С развитием интернет технологий сохранять нужный баланс становится все труднее. Риски слишком велики. Рано или поздно все стороны – и банкиры, и их клиенты - придут к однозначному выводу о необходимости отказаться от подобного рода проверки и искать новое, более надежное и безопасное средство. Это может быть сочетание мульти-факторной идентификации, одноразового пароля и биометрии.

«ПРО» для вашего дома

На сайте techhive.com 29 июня размещена статья Дж. Уидмана, посвященная защите жилого индивидуального дома. Автору присуще чувство юмора, когда он сравнивает эффективную систему охраны недвижимости с надежной противоракетной обороной.

Уидман предлагает рассматривать охрану жилища как сочетание разных прослоек защиты подобно одежде, которую мы последовательно на себя одеваем перед выходом на холодную улицу. Важно взглянуть на собственный дом глазами потенциального вора, который осматривает приглянувшийся объект с точки зрения соотношения риска и возможной добычи. И начинать надо с наружного осмотра: чем может привлечь мой дом злоумышленников? Это отправная точка для анализа, какие

системы и устройства нужны для крепкой и надежной защиты.

Различные охранные средства предназначены для разных задач. Сенсорные устройства для двери защищают внешний периметр, а детекторы движения – внутренние помещения. Видеокамера может быть использована как а) отпугивающее средство; б) сигнализация; в) криминалистический инструмент расследования в полиции и суде.

От базовых знаний он переходит к специфике. Важнейшее дело – определить, за что мы беспокоимся более всего, что для нас наиболее ценно. В зависимости от ответа на эти два вопроса и надо выстраивать архитектуру охраны. Есть ли у вас ребенок, с которого нельзя спускать глаз? Какую из комнат надо охранять пуще всего? А, может быть, главное – обеспечить защиту дорогой машины в гараже? Раздумывая над этими вопросами, нельзя упускать из виду окружающий ваш дом природный ландшафт и наличие соседей.

Если в вашем районе широко распространен взлом и угон автомобилей, надо позаботиться о видеокамере перед въездом-выездом. Если вас беспокоит в первую очередь жизнь и здоровье семьи, то целесообразно соединить сенсорные устройства на входных дверях и окнах с системой сигнализации. Некоторые сенсоры можно использовать для тревожного включения света внутри дома и снаружи при попытке несанкционированного проникновения. Сенсоры должны быть хорошо утоплены, невидимы для посторонних.

Сенсоры используются не только для защиты периметра. Если в одной из комнат хранится ружье, то можно встроить устройство, посылающее сигнал при открытии двери. Точно так же можно позаботиться и о подвальчике с хранящимся там (от детей подальше) вином.

Если дом часто пустует, не лишним будет позаботиться, что он выглядел так, словно там живут. Домушники обычно боятся света и признаков жизни. Поэтому было бы полезно использовать специальные лампы, которые бы время от времени включались и выключались по выбранной программе. Сначала включается лампа на первом этаже, потом на лестнице, через короткое время - в спальне. Так у наблюдателя извне создается впечатление о движении жильцов. Точно так же можно настроить включение и выключение телевизора.

Увлекаясь технологическими новинками, не забывайте о проверенных дедовских способах защиты дома. Позаботьтесь о надежных дверных замках, о том, чтобы во дворе не валялось ничего такого, с помощью чего можно было бы забраться в окно второго этажа.

На худой конец можно навесить фальш-камеры. Пусть дом выглядит как мощное укрепление и отбивает у преступников охоту залезть туда.

Базовые принципы охраны школ с помощью электронных СКУД

Всем очевидна насущная необходимость в надежной охране школьных учреждений, пишет Крис Уинн в статье Security Magazine (июньский выпуск за этот год).

Нередко при планировании программы охраны школ забывают о самых обычных преградах на пути потенциальных преступников. Крепкие и высокие заборы по периметру охраняемой территории служат достаточно эффективной помехой непрошенным гостям в любое время суток. Ворота и входные двери могут быть открыты или закрыты в зависимости от потока людей в разное время в течение учебного (рабочего) дня. Наконец, нельзя пренебрегать (при проектировании и строительстве) планировкой учебных и офисных помещений, коридоров и мебели.

В нынешние времена электронные СКУД превращаются в стандартные средства охраны школ, позволяющие держать под контролем, управлять доступом на территорию и в помещения родителей, учителей, административно-технического персонала, иных возможных посетителей. Проверка осуществляется через электронные базы данных, сформированные в системе. Если пропуск в порядке, система автоматически разблокирует вход и пропускает посетителя.

Взятые сегодня на вооружение системы СКУД напоминают действия традиционного охранника, который просматривает и сверяет удостоверение личности, впускает его обладателя, регистрирует факт посещения в специальном журнале. Автоматика действует быстрее, способна обслуживать за конкретный период времени намного больше людей, но, главное, мгновенно перекрывает все двери тем, у кого истек срок действия пропуска.

Электронная система эффективно управляет замками ворот и входных дверей, отдельных комнат и секций внутри здания.

Существуют разные виды электронного доступа. Это могут быть набираемые коды, карточки, прикладываемые к считывателям, специальные брелки. Некоторые системы используют биометрию – отпечатки пальцев или сканирование сетчатки глаз. Набирает популярность двух и многофакторная идентификация. К примеру, сочетание кода и электронного пропуска. Обычно такой способ применяется при охране особо важных помещений.

Огромное преимущество электронных систем перед обычными ключами проявляется в случае кражи или потери. Электронный пропуск просто деактивируется, заменяется новым. Нет необходимости менять замки, как это случалось в эпоху механических ключей.

Важно и то, что СКУД может управлять и другими функциями жизнеобеспечения здания. Например, лампы освещения включаются и выключаются автоматически в зависимости от времени суток и наличия в здании людей. Точно так же управляются единой программой системы отопления, кондиционирования, водоснабжения.

СКУД интегрируется с другими охранными технологиями – видеонаблюдением, тревожной сигнализацией, которые автоматически активируются в момент верификации пропуска. Если верификация дает негативный результат, камера начинает запись и трансляцию картинки с места инцидента, а тревожная сигнализация посылает сигнал в пункт охраны.

Как поддерживать хороший тонус у компьютерной группы реагирования на инциденты безопасности

Онлайновый журнал Chief Security Officer опубликовал статью Ст. Коллетт на тему управления командой квалифицированных айтишников, обученных реагировать на чрезвычайные ситуации в корпоративных сетях и компьютерах. Речь идет в первую очередь о первоклассных профессионалах, способных заранее предвидеть риски и угрозы, предотвратить или остановить хакерскую атаку, быстро восстановить работу сетей после компрометации. Такую команду трудно сформировать. Но еще труднее удержать.

Талантливые специалисты в области информационной защиты везде пользуются повышенным спросом. «Я чуть ли каждый день получаю предложения о новой работе», - рассказывает один крупный компьютерный инженер из Чикаго.

Руководители служб безопасности и информационной защиты делятся опытом удержания талантов в своих командах.

Предоставьте творческую свободу

Постоянно заглядывать через плечо и задавать вопросы, значит, мешать и раздражать подчиненных, утверждает Боранди, руководитель информационной защиты финансовой организации в Нью-Йорке. Его команда состоит из 8-10 специалистов в возрасте от 23 до 45 лет. Они решают множество задач: установка и эксплуатация межсетевых фильтров, контроль и управление приложениями безопасности, системами обнаружения взломов сетей, выявление уязвимостей, реагирование на инциденты безопасности. Каждому формулируется задача, которую они решают так, как считают нужным. В функции прямого начальника входит оберегать их от чересчур нервных менеджеров.

Дайте им те средства, инструменты, которые они хотят (в пределах разумного)

Нет универсального инструмента защиты, который бы нравился всем, считает Роб Уестервелт, аналитик из IDC (аналитическое агентство). Надо давать то, с чем им комфортно работать. Но чересчур много девайсов тоже плохо: слишком дорого и зачастую вносят хаос в работу группы. В банке First Financial Bank (штат Цинциннати) стараются избегать слова «нет», когда речь заходит о более совершенных и эффективных новинках. Профессионалам информационной защиты предоставляют возможность экспериментировать с новыми технологиями, правда, в разумных границах.

Прислушивайтесь к идеям, уважайте знания специалистов

Талантливые люди обычно стремятся расширить узкие рамки сформулированных задач, выйти на осмысление более широких проблем, влияющих на бизнес. Надо их внимательно слушать и адекватно реагировать на идеи и предложения. Они ценят такое отношение.

Используйте стимулы

Сложно стимулировать специалистов, на которых везде высокий спрос. Здесь следует подходить строго индивидуально, стараясь понять, что они считают для себя самым важным в своей жизни и работе.

Тренинг и обучение

Это тоже немаловажный компонент поддержания высокого тонуса команды. Ведь многие заинтересованы в преумножении своих знаний и умений. Поэтому надо предоставлять им возможность учиться, познавать новое в профессии.

Поощряйте конкуренцию

У членов команды должна быть возможность сравнивать себя с другими. Здоровое соревнование между ними помогает избавиться от пресыщения однообразной работой, но, главное, стимулирует профессиональный рост – а это именно то, что работодатель может реально предложить своим подчиненным, кроме зарплаты.

Как минимизировать проблемы, обусловленные человеческим фактором

В статье, размещенной 16 июня с.г. на сайте csoonline.com, рассматривается вопрос об ошибках, допускаемых персоналом при пользовании корпоративными сетями. Автор публикации И. Уинклер отмечает, что во всех сферах человеческой деятельности сбои, происходящие по вине людей, являются предметом повышенной озабоченности. Везде, кроме компьютерной отрасли. Почему-то, пишет Уинклер, в области информационных технологий человеческий фактор явно недооценивается.

К примеру, в авиации пилоты проходят тщательную предполетную медицинскую проверку. На промышленных предприятиях тратятся огромные деньги для предотвращения аварий. Размечаются зоны, где может работать строго ограниченное число людей, развешиваются предупреждающие и запретительные знаки, делается многое другое для охраны здоровья рабочих, обеспечения нормального производственного процесса.

Можно ли сказать то же самое относительно компьютерной безопасности? Нет, нельзя, утверждает автор. Огромное число сбоев в работе корпоративной сети, равно как и несанкционированных вторжений извне, происходит по причине непредумышленных ошибок со стороны персонала. В основе таких провалов – недостаток знаний, беспечность, невнимательность, подчас сознательное игнорирование инструкций.

Что касается повышения компьютерной грамотности пользователей, то для этого предназначены специальные тренинги, организуемые компанией. При этом важно не только показать, что и как надо делать, чтобы избежать ошибок, но в первую очередь

изменить поведение людей, привить им культуру безопасности.

Относительно невнимательности, несобранности, разгильдяйства дело обстоит сложнее. Пользователи хорошо знают, что можно, а что нельзя делать, но по рассеянности совершают глупейшие ошибки. Автор рекомендует в таких случаях вставлять в компьютерные программы и размещать на служебных местах предупреждения, тревожные знаки, постоянно напоминающие о мерах безопасности. Другой путь – моральное поощрение и материальная мотивация строго следовать букве и духу инструкций.

Теперь о тех персонажах, кто наплевательски относится к рекомендациям и запретам. К примеру, систематически используют один и тот же личный пароль для входа в служебные базы данных. Именно из-за такого отношения к служебным обязанностям хакеры получили доступ к конфиденциальной информации корпорации Сони и нанесли огромный материальный и репутационный урон. Автор статьи не видит иного способа бороться с недисциплинированными сотрудниками как с помощью кнута и пряника – наказанием и поощрением.

Фундаментальное решение проблем, связанных с человеческим фактором, лежит в программах повышения квалификации (awareness programs), чрезвычайно распространенных в западных компаниях. Применительно к области кибербезопасности такие программы предлагают обучение вопросам информационной безопасности (ИБ), повышение осведомленности об актуальных угрозах ИБ, о мерах и способах реализации атак и средствах защиты, фокусируют внимание сотрудников на важности обеспечения ИБ и т.п.

Автор статьи, будучи специалистом в области таких программ, подчеркивает необходимость изучать результативность тренингов, пути повышения их эффективности. При этом материальные и моральные стимулы играют первостепенную роль.

Снаряжение охранника

Редактор журнала Security Magazine Клэр Мейер опубликовала в июльском выпуске статью, посвященную снаряжению охранника.

Униформа

Униформа традиционно делится на строгую и облегченную, допускающую ношение неформальных элементов одежды. Главное, чтобы каждому, нуждающемуся в помощи, было легко распознать в толпе людей работника службы безопасности. Униформа также отражает имидж компании в глазах клиентов, партнеров, гостей.

По мнению Рика Ливайна,, вице-президента Sales for Uniform Market, руководителю СБ при выборе формы одежды следует руководствовать следующими главными факторами:

1. Распознавание – как легко могут служащие компании и гости идентифицировать охранника (офицера по безопасности).

2. Условия работы – наличие множества электрических приборов и проводов, быстровоспламеняющихся веществ, острых предметов, т.е. форма должна отражать опасности, с которыми может столкнуться охранник. Соответственно подбирается и форма, и материал, из которого она сшита.

3. Комфортность – иметь в виду, где будет работать охранник: внутри здания или снаружи, или здесь и там. Также имеет значение окружающая среда: одно дело – госпиталь, другое – университетский кампус.

При выборе формы обращать внимание на ее прочность, носкость, насколько она устойчива к многократной машинной стирке. Ливайн рекомендует использовать униформу, способную переносить до 50 стирок без потери формы.

Носимые при себе видеокамеры

Последний год отмечен дискуссиями в специализированной прессе относительно эффективности носимых камер. Филипп Калдуэлл, директор по безопасности госпиталя в городе Андерсон, штат Индиана, утверждает, что «лишний глаз» охране не помеха, а напротив, большое преимущество. Охранники госпиталя наделены полномочиями задерживать подозреваемых. В случае задержания хулигана или потенциального преступника носимые камеры чрезвычайно полезны в качестве видео и аудио свидетельства при дальнейшем разбирательстве. Многие руководители СБ рассматривают возможность обеспечения охранников мобильными камерами. Согласно опросу, проведенному недавно Security Management, 45% респондентов в лице глав СБ заявили, что планируют запросить у руководителей компании средства на закупку таких камер.

Дополнительное снаряжение

Кроме униформы и мобильного видеонаблюдения на рынке сегодня предлагается множество видов снаряжения для охраны. Их выбор зависит от ответов на следующие вопросы:

Каков характер рисков?
Должны ли охранники иметь оружие, и если да, то какие лицензии и тренинги для этого необходимы?
Могут ли возникнуть дополнительные задачи и проблемы во время дежурства?

Проверка удостоверений и пропусков на постах периметра охраняемой зона и во время патрулирования

Автор публикации рекомендует использовать для этой цели легкий по весу и удобный мобильный считыватель S3040. Высокое разрешение аппарата позволяет считывать и верифицировать фотографии на документах. Объем памяти составляет до 200 000 документов.

Специфика особо опасных зон

К ним можно отнести тюрьмы, удаленные охранные посты, другие условия, чреватые высоким риском нападения на охранников. В этом случае полезно применение трансмиттера фирмы Elpas – Lone Worker Transmitter, с помощью которого ведется отслеживание, навигация удаленных от пункта управления патрулей и охранных постов. Специальные тэги радиочастотной идентификации (RFID) позволяют с большой

точностью установить местонахождение охранника в случае нападения на него.

Книжное обозрение

Integrated Electronic Security: A Layered Approach
2/9/2015 by Martin Grigg; Reviewed by Terry L. Wettig, CPP

Автор книги имеет за плечами 25 лет работы в сфере технологий безопасности. Поэтому он со знанием дела рассказывает, как выбирать, устанавливать и эксплуатировать электронные охранные системы с наибольшей отдачей и результативностью.

Сегодня видеонаблюдение, системы электронного мониторинга – вещи обыденные, широко распространенные. Однако еще нередко встречаются случаи, когда устанавливаемая система охраны, отличная по характеристикам, не отвечает поставленным задачам, ожидаемым результатам.

Автор подсказывает, как избегать подобных ошибок. И делает это языком, понятным даже неспециалисту. Читатель найдет в книге много взятых из реальной жизни примеров правильного подбора и интеграции систем видеонаблюдения, СКУД, биометрических устройств для проверки и верификации. Книга полезна и интересна как новичкам в данной области, так и состоявшимся профессионалам.

Investigating Internet Crimes
by Todd Shipley and Art Bowker; Reviewed by Ben Rothke

Расследование и предупреждение киберпреступлений – дело очень сложное. Самый наглядный пример – взлом баз данных корпорации Сони хакерами извне в 2014 году.

Авторы книги предлагают читателю эффективную, как они считают, методологию расследования инцидентов безопасности и предупреждения подобных случаев. Излагаются фундаментальные основы, не только теоретические, но в первую очередь, непосредственно связанные с практикой.

Внимание читателей фокусируется на способах использования различных инструментов для расследований. При этом авторы призывают не зацикливаться исключительно на технологиях. Намного важнее знать, что делать, как реагировать на инциденты. На это и ориентирует читателей книга.

Книжное обозрение

Integrated Electronic Security: A Layered Approach
2/9/2015 by Martin Grigg; Reviewed by Terry L. Wettig, CPP

Автор книги имеет за плечами 25 лет работы в сфере технологий безопасности. Поэтому он со знанием дела рассказывает, как выбирать, устанавливать и эксплуатировать электронные охранные системы с наибольшей отдачей и

результативностью.

Сегодня видеонаблюдение, системы электронного мониторинга – вещи обыденные, широко распространенные. Однако еще нередко встречаются случаи, когда устанавливаемая система охраны, отличная по характеристикам, не отвечает поставленным задачам, ожидаемым результатам.

Автор подсказывает, как избегать подобных ошибок. И делает это языком, понятным даже неспециалисту. Читатель найдет в книге много взятых из реальной жизни примеров правильного подбора и интеграции систем видеонаблюдения, СКУД, биометрических устройств для проверки и верификации. Книга полезна и интересна как новичкам в данной области, так и состоявшимся профессионалам.

Investigating Internet Crimes
by Todd Shipley and Art Bowker; Reviewed by Ben Rothke

Расследование и предупреждение киберпреступлений – дело очень сложное. Самый наглядный пример – взлом баз данных корпорации Сони хакерами извне в 2014 году.

Авторы книги предлагают читателю эффективную, как они считают, методологию расследования инцидентов безопасности и предупреждения подобных случаев. Излагаются фундаментальные основы, не только теоретические, но в первую очередь, непосредственно связанные с практикой.

Внимание читателей фокусируется на способах использования различных инструментов для расследований. При этом авторы призывают не зацикливаться исключительно на технологиях. Намного важнее знать, что делать, как реагировать на инциденты. На это и ориентирует читателей книга.

Угрозы знают лучше, но по-прежнему ведут себя безответственно

Английская маркетинговая фирма Vanson Bourne провела глобальное исследование о том, как относятся служащие компаний к киберугрозам.

Опрошены 1 580 человек в разных компаниях. Четыре из пяти признались в том, что допускают на работе рискованные действия, хотя и понимают их последствия с точки зрения кибербезопасности. Только остальные 20% заявили, что ни при каких условиях не разрешают себе рискованных шагов.

«Мы не увидели положительных сдвигов в поведении работников, стоящих перед рискованным выбором, - говорит Х. Томпсон из компании Blue Coat Systems (программное обеспечение), которая спонсировала исследование. По иронии судьбы самые беспечные обнаружились в отделах информационных технологий (только 12% из них сказали, что не позволяют себе идти на риск).

Наилучшую осведомленность участники опроса продемонстрировали относительно

рисков, связанных с открытием файлов из неизвестных источников и просмотром порнухи с рабочих девайсов. 73% считают такие действия рискованными и очень рискованными. Только 2% не считают опасным открывать неизвестные файлы, а 3% - смотреть порносайты, используя офисные компьютеры.

Некоторые другие цифры.

65% считают опасным использовать несанкционированные приложения.
62% так же относятся к выгрузке неизвестных файлов из интернета.
56% понимают риски, обусловленные скачиванием видео, выходом с рабочих компьютеров в социальные сети.
46% знают о недопустимости погружаться в социальные медиа для личных интересов во время работы.
40% понимают, что рискованно использовать персональные мобильные устройства для служебных целей.

Тем не менее, во время работы 26% устанавливают несанкционированные приложения, 23% выгружают в офисные компьютеры неизвестные файлы, 31% просматривают видео, 41% выходят в социальные сети, 51% используют персональные мобильные девайсы.

(по материалам журнала Chief Security Magazine)