Охрана предприятия

№6 (40), 2014

Оглавление

Книжное обозрение

Fraud Analytics: Strategies and Methods for Detection and Prevention

Practical Aviation Security: Predicting and Preventing Further Threats, Second Edition

Исследования

Использование оружия в охране больниц

О некоторых ожидаемых тенденциях в сфере безопасности бизнеса в 2015 году

Онлайновый журнал Chief Security Officer (December 15, 2014) опубликовал прогнозы относительно развития мировой индустрии безопасности в 2015 году, сформулированные рядом исследовательских организаций, в частности компаниями Gartner, Forrester Research, RSA (подразделение корпорации EMC по обеспечению безопасности).

Выводы базируются в основном на данных анализа по США, но в ряде случаев отражают
глобальные тенденции. Вот некоторые из них.

Бюджеты предприятий охраны и корпоративных служб безопасности будут увеличиваться в основном за счет дополнительных капиталовложений в информационную защиту.

Ожидается растущий спрос на интегрированные технологии обнаружения рисков и угроз. Подъем обусловлен дальнейшим развитием т.н. «Интернета вещей» (Internet of things,), которое, в свою очередь, рождает все новые проблемы для защиты как цифровой, так и физической среды обитания.

Несмотря на рост ассигнований в системы распознавания хакерских взломов, все большее число частных компаний (по некоторых данным, до 60%), будут узнавать о компрометации их данных со стороны третьих лиц и организаций (партнеров, клиентов, блогеров, госорганов). А это, в свою очередь, негативно скажется на доверии людей к бизнесу.

Возрастут потери частного сектора от кибератак, организуемых на государственном уровне, в частности против энергетических объектов и других критически важных инфраструктур.

Будет наблюдаться определенная унификация языка информационной защиты, что в первую очередь связано с интегрированием данных по защите «Интернета вещей» в

технологии идентификации угроз корпоративным сетям.

Дискуссии и споры вокруг соблюдения прав и невмешательства в частную жизнь (privacy) будут носить более прагматичный, сбалансированный характер. Прогнозируется дальнейшее совершенствование национальных и международных законодательств, обеспечивающих защиту таких прав. Соблюдение прав личности будет играть возрастающую роль в качестве конкурентного преимущества.

Как ожидается, в 2015 году значительно увеличится количество смартфонов и иных «умных» гаджетов (по мнению ряда исследователей, на 30%), соответственно, возрастут и риски.

Хотя ритейлеры останутся главным объектом хакерских атак, преступники будут уделять больше внимания кражам персональных данных в таких сферах как здравоохранение.

Продолжится тренд расширения онлайн банкинга и интернет торговли, особенно среди молодых поколений, сопровождаемый попытками производителей соответствующих технологий делать их более безопасными, эффективными и доступными в управлении.

Технологии безопасности снижают риски на спортивных соревнованиях

Теракт во время Бостонского марафона заставил руководителей спортивных организаций и стадионов ужесточить меры безопасности. Этому вопросу посвящена статья в журнале Security Magazine (October 1, 2014).

Повсеместно внедряются металлодетекторы, переписываются инструкции и политики безопасности. Службы охраны используют широкий набор технологий и методов снижения риска для болельщиков, спортсменов, персонала спортивных сооружений во время проведения соревнований.

В комплексе мер самое серьезное значение отводится социальным сетям. По мнению экспертов, внимательный мониторинг наиболее популярных у болельщиков форумов и чатов позволяет на раннем этапе, еще до соревнований, понять, откуда и какие исходят угрозы. Некоторые специалисты уверены, что такой мониторинг следует проводить до начала, во время и по завершении спортивных событий.

Получают распространение программные продукты, позволяющие моделировать разные ситуации (simulation software), в частности, прорабатывать различные варианты заполнения стадиона зрителями, организации их выхода, а также эвакуации в случае возникновения экстремальных условий.

На территории крупных спортивных комплексов сооружаются телефонные будки, где посетители могут зарезервировать себе места на трибуне, воспользоваться картой комплекса, а также обратиться за помощью к службе безопасности в случае опасности.

Система видеонаблюдения усиливается за счет аналитики, детекторов движения, различных сенсоров, с помощью которых охранники мгновенно переключают внимание на те сектора, где завязывается конфликт, фиксируется неадекватное поведение болельщиков.

Создаются общенациональные, доступные спортивным организациям и клубам хранилища данных, куда стекается важная с точки зрения безопасности информация (например, о правонарушениях, конкретных злоумышленниках и т.п.).

Повсеместно внедряются цифровые двусторонние радиопередатчики. Они особенно полезны, когда возникает срочная необходимость отправить на место происшествия находящегося поблизости охранника.

Все большую популярность завоевывают программные продукты, распознающие и запоминающие государственные номера автомобилей, заезжающих на паркинг при спортивном комплексе. Таким способом «вылавливаются» болельщики, которым запрещено посещение спортивных соревнований.

Обязательным элементом охраны спортивных комплексов и стадионов являются программы подготовки персонала. Они предусматривают регулярный просмотр и анализ видеоматериалов, фиксирующих те или иные нестандартные ситуации во время проведения реальных соревнований.

Охрана небоскребов. Технологические тенденции

(продолжение статьи, опубликованной в выпуске №39)

Еще десяток лет назад работники службы безопасности высотки Willis Tower (110 этажей, г. Чикаго) в письменной форме составляли и отправляли начальству свои замечания и отчеты. Недавно охранников оснастили iPad Minis с камерами. Теперь все донесения формируются и доставляются в электронной системе управления данными, которая также служит хранилищем всей важной информации, такой, например, как планы действий в чрезвычайных обстоятельствах. Данная система экономит массу сил и времени, которые ранее растрачивались на чисто административные цели.

Одновременно запущена и функционирует система регистрации, учета и контроля посетителей (visitor management security system). В небоскребе мощный поток людей: 13 000 работающих в офисах плюс ежедневно 2 000 посетителей и гостей. Можно представить себе заторы на входных дверях в часы пик, особенно когда кто-то забывает дома или теряет свой пропуск – а это частенько случается по понедельникам, пятницам, а также в первый день после праздников. Новая система разгрузила работу охранников. Для рассеянных клерков имеется специальное устройство при входе в здание, работающее в режиме реального времени – терминал самостоятельной регистрации. Терминал проверяет введенные данные и автоматически выдает временный пропуск.

Также существенно облегчена работа с деловыми посетителями. Им заблаговременно высылается по электронной почте специальный штрих-код, с помощью которого они

становятся обладателями пропуска. В ближайшем будущем планируется использование смартфонов в качестве электронных пропусков.

Другое направление развития технологий безопасности учитывает особенность небоскребов, а именно – их устремленность вверх (в США небоскребом считается любое здание высотой более 75 футов, т.е. примерно 7 этажей и выше). Главная проблема – помощь людям на верхних этажах в случае возникновения экстремальной ситуации (пожар, теракт и т.п.). Поэтому такое огромное внимание уделяется составлению специальных планов эвакуации, а главное – обучению работающего в высотке персонала действиям, которые необходимо предпринимать в случае опасности. Обычно такие учения проводятся раз в год. В Нью-Йорке службы безопасности некоторых небоскребов организуют тренировки ежеквартально. На занятиях демонстрируют учебные видео, комментируют их и обсуждают, отвечают на вопросы.

Проблема сложнее в жилых корпусах. Нередко резиденты спохватываются только при сигнале тревоги, не зная, что предпринимать, мечась из стороны в сторону, создавая хаос и сея панику. Некоторые вовсе отказываются покидать свое жилище, невзирая на опасность. Во время смерча Sandy такое поведение стало причиной гибели нескольких человек.

Тем не менее, системы безопасности в жилых высотках постоянно совершенствуются. Внедряются более эффективные противопожарные и сигнальные устройства. Предусматриваются дополнительные возможности для быстрой эвакуации с верхних этажей.

Фантастическими, на первый взгляд, кажутся некоторые проекты, устремленные в будущее. Так, в частности, серьезно обсуждается и прорабатывается возможность замещения дежурных охранных патрулей дронами (беспилотниками).

Три важнейших вопроса в заявке на финансирование программы охраны предприятия

Эта тема довольно подробно развернута в публикации М. Сантарканжело на сайте csoonline.com (November 7, 2014).

Автор выделил три вопроса, которые, по его мнению, необходимо учитывать руководителю корпоративной СБ при составлении заявки на финансирование.

Безотлагательность и приоритетность программы

Первые лица любой компании обычно имеют дело с рядом финансовых запросов от разных отделов и направлений бизнеса. При этом каждая заявка аргументируется как «абсолютно приоритетная». Руководителю приходится выбирать, принимать решение, как правильно выстроить бюджет организации, распределить средства.

Прежде всего, автору заявки надо четко сформулировать для себя вопрос: «что мы

можем предложить, чтобы убедить руководство принять верное решение?». Зачастую представляется длинный список инициатив, проектов на выбор руководству. Такой список может включать и 20, и 50 проектов. Это крупная ошибка. Работая над заявкой, необходимо ограничиться не более 3 программами (проектами), и на них сконцентрировать всю аргументацию, включая основательные доводы в пользу безотлагательности и приоритетности.

Сравнение с конкурентами

В конкурентной борьбе никто не хочет отставать, в том числе и в сфере новых технологий. Однако, погоня за новейшими программными решениями чревата повышенными рисками. Самые последние технологии, как правило, дороги и не всегда гарантируют высокий результат. Вопросы безопасности, пишет автор, это «спокойный бизнес» - в том смысле, что не надо стремиться обогнать всех и каждого. В любом случае требуется время, чтобы собрать данные о той или иной новинке, чтобы понять, насколько она оправдывает затраты и минимизирует риски. Предпочтительно не бежать впереди всех, но без спешки определить правильный баланс между инвестиционными рисками и реальными результатами.

Если же вы предлагаете нечто новое для данного рынка, то позаботьтесь, чтобы тот, кто принимает решение, был вооружен убедительными доводами в пользу проекта – эмоциональными, логическими, финансовыми.

Сумма запрашиваемых средств и измерение конечных результатов

Речь идет о существенном вопросе: «что компания получит в обмен на затраченные средства?». Предприниматели и топ менеджеры обычно обладают более широким взглядом на проблему рисков, чем специалисты в области технологии или безопасности. Это не означает, что они ждут от вас подробных разъяснений по проекту и сложных калькуляций. Им просто надо понять, как предлагаемый вами проект или программа решает конкретную проблему.

Поэтому в заявке на финансирование необходимо отразить следующие позиции:

- Как проект соотносится с решением проблемы
- Каково ожидаемое влияние на работу организации (работать будет сложнее или, напротив, проще, и т.п.)
- Сколько времени понадобится на осуществление проекта
- Какие усилия потребуются, включая другие команды и подразделения, вовлеченные в проект
- Насколько мы уверены в успехе проекта

Короче говоря, ваша заявка должна убедительно продемонстрировать, как требуемые финансы, время и трудовые ресурсы решат проблему. Чем вы точнее в оценках и деталях, тем больше шансов на одобрение.

Семь роковых ошибок в вопросах безопасности нового бизнеса

Эксперты обращают внимание, что организаторы новых бизнесов (стартапов) зачастую пренебрегают вопросами охраны предприятия, безопасности бизнеса. С. Раманан, автор статьи в журнале Chief Security Officer (November 10, 2014), называет семь, наиболее частых, по его мнению, просчетов, которые допускают предприниматели.

Непонимание угроз для бизнеса

Статистика свидетельствует, что почти 90% малых предприятий в США подверглись компрометации корпоративных сетей за последний год, но только каждый десятый из них обнаружил утечки важной информации. Автор настоятельно рекомендует продумывать систему информационной и физической охраны интеллектуальной собственности еще до запуска нового бизнеса. Осуществлять предварительный анализ возможных рисков, определять конфигурацию защиты.

Отсутствие ИТ стратегии

ИТ стратегия предполагает, что вы ясно понимаете и знаете, где разместить корпоративный сервер, где и как хранить конфиденциальную, служебную информацию. Случается, что организаторы стартапа поначалу полагаются на облачные исчисления, заключают соглашение с третьей стороной, но спустя какое-то время, уже потратив немалые средства, приходят к выводу, что эффективнее и безопаснее хранить все корпоративные данные у себя в офисе. Теряется драгоценное время. Впустую тратятся деньги.

Отсутствие контроля безопасности в отношениях с «облачным» партнером

Большинство новых малых предприятий в США предпочитают хранить данные в «облаках». Здесь решающую роль играет выбор партнера. Главный критерий – забота «облачной» компании об информационной безопасности клиентов. Правильный и своевременный выбор партнера убережет стартап от многих неприятностей.

Пренебрежение проверками на безопасность в процессе непрерывного обновления защитных программ

«Непрерывное обновление» или «непрерывная подписка на программы» (continuous deployment) разъясняется экспертами как “процесс, по которому программное обеспечение, включая антивирусы, обновляется несколько раз в день: минуты в противовес дням, неделям или месяцам”. Подробнее см. http://agilerussia.ru/practices/continuous-deployment-practice/
Неверный выбор инструментов информационной зашиты

Неверный выбор программы

Начиная новый бизнес, важно не ошибиться в выборе программных продуктов, которые бы в максимальной степени отвечали специфике бизнеса и обеспечивали надежную информационную защиту. Критически важно учитывать мнение специалистов в данной области.

Игнорирование роли персонала в защите интеллектуальной собственности

Важный фактор информационной защиты – умение быстро выявить проблему в сети и устранить ее. Кто способен это делать? Конечно, в первую очередь, сотрудники компании как постоянные пользователи корпоративной сети. Их необходимо

стимулировать, мотивировать, добиваясь незамедлительной реакции на признаки взлома и иных видов компрометации в форме своевременного доклада без всякой боязни понести наказание за те или иные «проколы». С самого начала надо учить персонал умению идентифицировать нарушения и инциденты безопасности.

Неумелое использование программ «bug bounty»

Программа «bug bounty» - программа финансового вознаграждения сотрудников компании за нахождение уязвимостей в программном обеспечении. Чтобы не подвергнуться потоку обнаружений во имя материального вознаграждения, необходимо классифицировать все потенциальные уязвимости, четко определив, какие из них не приемлемы и подлежат устранению.

Почему незаменима собственная служба информационной безопасности?

Онлайновый журнал Chief Security Officer (November 25, 2014) опубликовал дискуссионный материал на тему, что лучше – пользоваться услугами сторонней организации или создавать собственную службу информационной защиты? Судя по статье, журнал склоняется ко второму варианту.

В принципе все функции, связанные с информационными технологиями, могут быть отнесены на популярный сегодня аутсорсинг. Но прежде чем делать выбор, надо хорошенько подумать, какой из вариантов наиболее надежен и эффективен.

Какими бы талантами ни обладал специалист аутсорсинга, он никогда не сможет полноценно заменить штатного сотрудника. Даже если сторонний эксперт будет регулярно посещать клиентскую организацию, изучать ее специфику и особенности, все же предпочтительнее собственный специалист, который помимо чисто профессиональных функций «привязан» к организации, кровно заинтересован в результатах бизнеса, в репутации своей «конторы».

Помимо морального аспекта играет роль и фактор быстрых технологических изменений, затрагивающих непосредственно интересы всей организации, и неизбежность внутренних изменений в компании под влиянием перемен во внешней среде, в результате переориентации в стратегии и тактике бизнеса, по причине множества других меняющихся обстоятельств. Понятно, что постоянному работнику намного легче ориентироваться в происходящих переменах, адекватно на них реагировать, корректируя или тонко настраивая управляемые им технологии.

Преимущества собственной службы информационной защиты особенно наглядно проявляются, когда происходит взлом, компрометация корпоративной сети, утечка данных. Размер ущерба напрямую зависит от быстроты обнаружения и скорости реагирования. В таких обстоятельствах превосходство внутренней службы перед сторонней организацией очевидно. Свои специалисты досконально знают архитектуру и среду, в которой функционируют информационные технологии, а потому как никто

извне могут быстро и эффективно минимизировать ущерб.

Конечно, нельзя отрицать значение привлечения профессионалов со стороны. Будучи узкими специалистами, они могут помочь в развитии конкретных технологических функций, представить свежий, «незамыленный» взгляд на состояние и дальнейшие перспективы информационной защиты в вашей компании. Они могут быть полезными с точки зрения применения опыта, наработанного в других компаниях. Наконец, приглашенные профессионалы весьма эффективны при испытании систем безопасности на предмет слабостей, уязвимостей, которые не всегда заметны изнутри.

При всем при этом, подводит итог журнал, безопасность – эта цена, которую обязан платить бизнес, рассчитывающий на успех. Нельзя эффективно защитить бизнес, опираясь исключительно на консультантов и арендованные технологии. Нужны собственные квалифицированные кадры.

Беспроводной интернет – причины для беспокойства

Компании требуют от своих сотрудников высокой эффективности, где бы они ни находились в рабочее время. Этому запросу отвечают технологии беспроводного Интернета и развитие Wi-Fi. Между тем, профессионалы по вопросам безопасности бьют тревогу, утверждая, что бесконтрольное пользование публичными сетями Wi-Fi чревато серьезными негативными последствиями. Хакеры уже давно освоили Wi-Fi для своих злонамеренных целей.

Стивен Чабински в октябрьском выпуске журнала Security Management, рассуждая на эту тему, приводит такой пример. Двоих парней арестовали после того, как они, находясь в салоне своей машины в автопаркинге и пользуясь бесплатным Wi-Fi, залезли в хранилище данных сети строительных магазинов в шести штатах США, овладели персональной информацией многих тысяч людей. Автор статьи подчеркивает, что коммуникации Wi-Fi легко взламываются с помощью самого простого программного продукта. Злоумышленники получают в свое распоряжение незашифрованные данные, но также научились вскрывать и слабо зашифрованную информацию.

Перед компаниями, в первую очередь небольшими, стоит дилемма: изыскивать немалые средства на новейшие шифровальные протоколы WPA2, предназначенные для предприятий и организаций, либо обходиться более дешевыми, но менее безопасными «домашними» стандартами информационной защиты (межсетевыми фильтрами, пин-кодами и т.п.). Решение показывает, насколько далеко компания готова идти в обеспечении своей безопасности при пользовании сетями Wi-Fi.

Сегодня рынок предлагает разные средства безопасности, включая технологии, позволяющие одновременно пользоваться несколькими, не связанными между собой сетями (зонами) Wi-Fi, предназначенными для специфических групп пользователей (собственный персонал, посетители, поставщики, партнеры, клиенты и даже раздельные конференц-залы).

Конфигурация корпоративной сети Wi-Fi зависит и целиком определяется особенностями организации. К примеру, одна замкнутая зона - для младшего персонала, отдельные зоны – для среднего и командного уровней менеджмента. Эксперты рекомендуют одновременно использовать современные системы шифрования, встроенные в корпоративный сервер и доступные только сотрудникам фирмы, обладающим соответствующими паролями и пин-кодами.

Штатные специалисты ИТ отдела также должны иметь полномочия регулировать пользование Wi-Fi, например, прерывая при необходимости коммуникации между компьютерами, между ними и принтером.

Безотносительно от метода идентификации, принятой в компании, важно предупредить возможные попытки сотрудников в обход корпоративных правил настроиться на чужие зоны Wi-Fi. . Есть технологии, обнаруживающие подобные трюки и помогающие находить «хулиганов». Кроме того, необходимо проводить с персоналом тренинги, раскрывая риски, связанные с использованием иных, не родных корпоративных сетей Wi-Fi.

Важно предупредить командируемых за границу или по стране о повышенной осторожности в отношении гостиничного Интернета. Предоставляемые отелями возможности Wi-Fi обычно вполне легитимны, но зачастую кишат хакерами, способными украсть ваши пароли, персональные данные, финансовую информацию и внедрить в компьютеры зловредные вирусы.

Бэкграундные проверки иностранных граждан и безопасность бизнеса

В статье на эту тему (веб-сайт securitymagazine.com, October 1, 2014) речь идет главным образом об американских компаниях, нанимающих нерезидентов. Но основные оценки и выводы вполне универсальны, приемлемы и для других стран, вовлеченных в процессы мировой глобализации экономики и бизнеса.

Дефицит квалифицированных кадров – проблема не одной только Америки. Она вынуждает многих бизнесменов обращаться к зарубежным рынкам труда. Помимо закрытия узких мест в кадровой политике привлечение иностранцев, воспитанных в иной культуре, способствует диверсификации подходов к решению деловых вопросов, обогащению мировым опытом.

Но при этом ключевое значение имеет проверка соискателей. По опросам, проводившимся в США, примерно треть компаний пренебрегает проверкой образовательного уровня, криминальной истории, деловой и моральной репутации на прежнем месте работы. Такое отношение чревато не только ошибками в определении реальной квалификации, но и рисками для безопасности бизнеса.

Причины, по которым работодатели игнорируют тщательные глобальные проверки, разнообразны. Чаще всего они исходят из того, что такие проверки нужны и возможны лишь при наличии зарубежных филиалов и отделений, а также «дочек». Между тем, подход должен учитывать те задачи, которые ставит компания, включая обеспечение

безопасности бизнеса. Эксперты рекомендуют исследовать риски, которые угрожают бизнесу без проведения тщательных кадровых проверок на международном уровне.

Что дают в реальности рекомендуемые проверки?

А. Подтверждение опыта, знаний и навыков претендента на работу. Некоторые соискатели убеждены, что их будущие работодатели не будут затрудняться основательной проверкой представленного резюме, а потому легко фальсифицируют данные об образовании, прежней работе. Еще один довод в пользу проверки – наличие во многих странах т.н. «мельниц» по фабрикации фальшивых дипломов и удостоверений.

Б. Универсализация кадровой политики и практики. К примеру, на одно место претендуют два кандидата, один с дипломом местного университета, другой – с дипломом зарубежного ВУЗа. Может случиться, что компания удовлетворится проверкой одного лишь отечественного учебного заведения. Тогда со стороны второго кандидата могут последовать обвинения в дискриминационной кадровой политике (в США такие дела рассматриваются в судебном порядке). Поэтому эксперты настоятельно советуют равное отношение к наведению справок по всем соискателям.

Специалисты также рекомендуют:

Проводить проверки в соответствии с нормами и законами той страны, которую представляет кандидат. Они различаются от государства к государству. В одних странах хранение персональных данных в компаниях после увольнения сотрудника запрещено, в других строго регламентировано по времени и способам использования. Эти особенности необходимо знать в каждом конкретном случае.

Стараться понять чужую культуру. Пример из реальной жизни. Работодатель, отвечая на запрос из-за рубежа относительно одного из его работников, солгал, заявив, что «его не знает, и что тот никогда у него не работал». Он так поступил, следуя местной традиции, обычаям. Не более того.

Автоматизировать процесс проверки. Программные продукты, облегчающие поиск данных на глобальном уровне, существуют и продаются. Это специальные приложения с поисковыми функциями, позволяющими проверять если не всю, то существенную часть информации, в частности, криминальное прошлое, паспортные данные.

Почему информационная защита зависит от физической охраны

В современную эпоху кибервойн и киберкриминала принято считать, что электронные средства защиты интеллектуальной собственности вытеснили меры физической защиты информации. С таким подходом не соглашается Микаэль Оберлендер, опубликовавший на эту тему статью в онлайновом издании Security Magazine (September 9, 2014).

Он приводит историю, случившуюся с ним во время авиарейса. Свой мобильный

телефон он положил на соседнее свободное место. В момент приземления самолет крепко тряхнуло, телефон оказался на полу, затем прокатился по наклонному полу вдоль рядов до салона первого класса, где его подобрала стюардесса. Мобильник имел пин-код и был защищен шифром. Единственная информация, высветившая на экране, указывала на имя владельца и номер данного аппарата. Сверившись со списком пассажиров, стюардесса без труда отыскала автора статьи и вернула телефон.

По мнению Оберлендера, этот случай убедительно свидетельствует в пользу значимости не только информационной (пин-коды, шифрование и прочие способы), но и физической защиты (в данном конкретном случае речь идет о необходимости держать аппарат в надежном месте, при себе, под неусыпным контролем).

Автор приводит еще несколько примеров пренебрежения мерами физической охраны. В одном случае говорится о свободном, неконтролируемом доступе в помещение, где хранятся электронные данные при соблюдении строжайших мер информационной защиты. В другом – о разбросанных в подвальном помещении (автомобильном паркинге) коммуникационных кабелях, легко доступных для любого злоумышленника.

На основе множества подобных фактов автор делает заключение о необходимости продуманно выстраивать охрану интеллектуальной собственности, начиная с мер физической защиты и заканчивая самыми изощренными методами информзащиты. И эту работу надо проводить уже на этапе планирования. Вот несколько его рекомендаций:

Всегда рассматривайте и анализируйте несколько разных конфигураций физической и электронной защиты, выбирая вариант, который наиболее подходит к вашим специфическим задачам и условиям.

Наилучший вариант - сочетание физических и информационных мер защиты интеллектуальной собственности.

Организуя хранилище данных или любую другую информационную инфраструктуру, проверьте всевозможные слабости и уязвимости не как инженер, а как злоумышленник. Все физические подходы к оборудованию должны быть закрыты для посторонних, находиться под строгим контролем.

Не пренебрегайте охраной периметра. Надежно перекрывайте возможные пути и способы несанкционированного проникновения.

Что касается СКУД, то здесь важно не забывать о физической защите электронных пропусков, не допускать их несанкционированной передачи от одного лица к другому, своевременно реагировать на кражу или потерю.

Не забывайте о необходимости обучать и тренировать не только сотрудников СБ, но и пользователей информационных технологий на всех уровнях организационной структуры.

О некоторых базовых принципах охраны вестибюля (лобби)

О некоторых базовых основах охраны лобби напоминает С. Людвиг в публикации журнала Security Magazine за ноябрь текущего года.

Оценка безопасности

Первый шаг на пути создания эффективной программы охраны – оценка слабостей, брешей, уязвимостей, ведущих к несанкционированному проникновению в охраняемую зону. Причем, такой анализ необходимо повторять регулярно, с учетом изменения среды и технологий. Также важно осуществлять анализ и оценку потенциальных рисков и возможных потерь. Такие риски рассчитываются с точки зрения возможности и вероятности несанкционированного вторжения. С учетом проведенного анализа предположительных ситуаций формируется конфигурация охранной системы.

Назначение лобби

В зависимости от назначения охраняемого помещения выбирает тип системы безопасности. Идет ли речь о компании с высоким трафиком персонала и гостей? Или бизнес в основном носит «внутренний» характер и не предполагает большого числа визитеров и перемещений сотрудников? Если число ежедневных посетителей «зашкаливает», то, очевидно, имеет смысл устройства системы двойных дверей. Работающие в здании с помощью электронных пропусков беспрепятственно проходят через обе двери, расположенные друг от друга на определенном расстоянии, в то время как посетителей охранники встречают, проверяют, выдают временный пропуск сразу же после прохождения первой, внешней двери.

Дизайн

Правильный дизайн вестибюля имеет большее значение, чем обычно полагают люди. От расположения рецепции, пункта охраны зависит, насколько легко можно проникнуть в служебные помещения. В идеале должна действовать система двойных входных дверей с размещением охраны между ними. Для усиления безопасности рекомендуется, чтобы принимающая сторона там же встречала гостя и провожала до места официальных переговоров. Эксперты также советуют размещать конференц-залы, переговорные комнаты на первом этаже, рядом с вестибюлем таким образом, чтобы посетитель не имел возможности без разрешения слоняться по этажам и служебным помещениям.

Система регистрации, учета и контроля посетителей организации

Система включает терминал самостоятельной регистрации, который сканирует удостоверение посетителя, регистрирует и выдает пропуск (бэджик). Все данные хранятся в памяти системы, поэтому можно легко определить, кто находится в здании в любой данный момент, кто пришел и как долго пребывает в здании, как часто тот или иной визитер посещает организацию. Такая информация исключительно ценна при возникновении экстремальной ситуации. Для правильного пользования такой системой формулируются соответствующие инструкции и политики, охранники

проходят обучение. Все чаще такие системы дополняются камерами видеонаблюдения, видеоаналитикой, позволяющей контролировать число посетителей, находящихся в здании. Наиболее совершенные системы видеонаблюдения включают специальные сенсоры, детекторы движения, сигнализирующие об угрозах при определенных обстоятельствах.

О чем надо помнить, отправляясь в новогоднее путешествие

О мерах предосторожности во время отпускных путешествий пишет Г. Хатчимонжи в онлайновом издании Chief Security Management.

Все более возрастающее число людей становятся жертвами хакеров и грабителей в результате размещения информации о своих планах в Интернете. Особенно опасно оповещать о своих планах в социальных сетях, подчеркивает автор. Злоумышленники легко высчитывают, когда и на какое время покидают пользователи соцсетей свои дома.

Другая проблема связана с использованием мобильных устройств. Автор предупреждает о необходимости относиться к своему гаджету столь же внимательно и осмотрительно, как к кошельку. Сегодня мобильные устройства многофункциональны. Они служат ключами от дома и автомашины, хранят данные кредиток, контролируют и управляют домашним хозяйством на расстоянии…. Поэтому так важно все время держать их при себе, не оставлять без внимания и контроля. Тем более, что сегодня воры технически подкованы, хорошо знают, как обезопасить украденный смартфон или айфон от стирания информации. Для этого достаточно держать гаджет вне зоны Wi-Fi, не подключать его к веб-сети.

Готовясь к путешествию, важно руководствоваться обычным здравым смыслом. Прежде всего, выбирать места, более-менее безопасные с точки зрения криминала. Во время поездки желательно не включать без особой на то надобности телефон в публичных местах (кафе, аэропортах, железнодорожных станциях), где есть Wi-Fi. Это зоны повышенного риска. Также необходимо проявлять осторожность при подключении смартфона (айфона) к публичным интернет сетям. Дело в том, что хакеры наловчились создавать (имитировать) собственные зоны Wi-Fi в кафе и прочих публичных местах, легко получая доступ к данным, хранящимся на вашем смартфоне, при подключении.

Автор также рекомендует во время путешествия не привлекать к себе излишнего внимания как к туристу. Есть масса признаков, которые отличают путешественника от местных жителей: карты и путеводители в ваших руках, необычная для данного места одежда, вопросы к прохожим о том, как и куда пройти… Если вам необходимо получить информацию, то лучше всего для этого зайти в приличный магазин или обратиться в полицейский участок. Если надо добраться из пункта А в пункт Б, то возьмите такси – лучше заплатить, чем подвергаться риску ограбления.

Важно не забывать простые меры предосторожности. Например, всегда держать бумажник во внутреннем кармане, паспорт, деньги и драгоценности хранить в сейфе

отеля.

Многие связывают угрозы для мобильных компьютеров и сотовых телефонов исключительно с работой хакеров в сети. Это неверно, подчеркивает автор публикации. Опасность тривиальной кражи гаджета велика, если вы оставляете его без присмотра на пляже, в ресторане, ином публичном месте.

В любом случае настоятельно рекомендуется шифровать все данные на мобильных устройствах. Нельзя забывать и о пин-кодах. Они должны быть буквенно-цифровыми и содержать не менее 10 знаков. Это не гарантирует от взлома на все 100%, но осложнит и замедлит работу хакера.

Автор предостерегает от использования зоны Wi-Fi в гостиничном номере, т.к. она легко доступна злоумышленнику. То же самое можно сказать и о бизнес-центре отеля (если таковой имеется): высок риск, что вся информация, которую вы набираете на компьютере отеля, сохраняется в его памяти и может быть использована против вас.

Эксперты советуют избегать по возможности персонально идентифицируемой информации при пользовании публичными сетями.

Как ухаживать за бронежилетом. Четыре рекомендации

Канадский онлайновый журнал Canadian Security Magazine опубликовал заметку, подсказывающую, как хранить и использовать бронежилет в наилучшем состоянии (October 19, 2014).

Тщательная чистка

Не допускайте полного погружения бронежилета в воду. Вода способна повредить, если не разрушить защитные свойства изделия. Вместо стирки тщательно чистите с помощью намыленной губки и теплой воды. После этого положите сушиться в хорошо вентилируемое место, но ни в коем случае не используйте обычную вешалку из комода. Храните подальше от солнечных лучей, которые при продолжительном воздействии негативно влияют на специальный материал, из которого сделан бронежилет. То есть не сушите изделие на открытом воздухе под солнцем.

Не используйте поврежденный бронежилет

При выборе бронежилета обращайте внимание на признаки повреждения в результате последнего по времени использования. Дырки от пуль, порезы снижают уровень защищенности. Выбирайте изделие, в котором будете чувствовать себя уверенно и надежно. Не жалейте времени на осмотр.

Используйте бронежилет точно по его назначению

В принципе существует универсальная защита от различных поражающих средств. Но преобладающее большинство изделий предназначено для защиты от определенного вида оружия. К примеру, бронежилет, защищающий от пуль, мало подходит для

защиты от холодного оружия. И наоборот. По этой причине, всякий раз выбирайте такой тип бронежилета, который в наибольшей степени соответствует специфике предстоящего дежурства, наиболее вероятным угрозам.

Главное – в правильной подготовке

Всегда надо быть готовым к любым неожиданностям. Независимо от того, в какой раз вы выходите на дежурство в обычно спокойном месте, нельзя на все 100% исключать попытки вандализма, грабежа, несанкционированного вторжения. Поэтому носить бронежилет никогда не мешает. Вы сами выбираете, какой бронежилет брать: легкий, под верхнюю одежду, или, напротив, поверх рабочего костюма, демонстрируя тем самым потенциальному злоумышленнику, что готовы к любому повороту.

Внимательно изучайте внешних консультантов и партнеров

Модный ныне аутсорсинг предполагает приглашение к сотрудничеству исследовательских структур, рекрутинговых фирм, консалтинговых организаций.

Основатель и глава Security Management Resources (SMR Group) Джерри Бреннан и руководитель консалтинговой компании Mattice and Associates Линн Маттис опубликовали в журнале Security Magazine (October 1, 2014) статью, призывающую предпринимателей и менеджеров тщательно изучать и проверять потенциальных партнеров, прежде чем подписывать с ними контракт. Надо задать себе и попытаться ответить на такие вопросы:

- Действительно ли нам известна репутация потенциальных партнеров, принятая и соблюдаемая ими профессиональная этика, прежний опыт работы с компаниями и людьми?
- Знаем ли мы достаточно хорошо, как они будут управлять, хранить и использовать нашу корпоративную информацию?
- С кем они будут делиться служебными данными?

Несколько реальных примеров:

Одна известная крупная компания пригласила консультанта, представившего весьма впечатляющее резюме, а, кроме того, имевшего опыт работы в глобальной исследовательской корпорации. Между тем, консультант был замешан в крупном скандале в связи с кражей интеллектуальной собственности у прежнего работодателя, расследованием занималось ФБР. Уже работая на новом месте, он был осужден федеральным судом по четырем пунктам обвинения.

Среднего размера фирма, специализирующаяся в области информационной защиты, наняла консультанта, который, как оказалось, незадолго до этого был уличен в мошенничестве. Любопытно, что руководство фирмы, узнав об этом, ограничилось разговором с новым сотрудником и вполне удовлетворилось данными им разъяснениями. И он продолжал работать.

Подобных примеров, пишут авторы статьи, пруд пруди. Привлеченных консультантов

уличают в незаконном владении и злоумышленном использовании информации и продукции работодателей, в том числе данных о клиентах, стратегических планах, маркетинговых проектах и прочих закрытых аспектах корпоративной деятельности.

В последний год авторы публикации обсуждали эту проблему со своими клиентами, в частности, интересовались, готовы ли они принять к себе на работу специалиста с подмоченной репутацией, подозреваемого в совершении неэтичных действий. Все полученные ответы четко разделяются на две категории.

Первые категорически против каких-либо контактов с теми, кто не соблюдает профессиональную этику, не говоря уже о правонарушителях.

Вторые готовы поступиться принципами, ссылаясь на острую конкуренцию и дефицит квалифицированных кадров.

Последняя позиция не вызывает у авторов статьи удивление. Они считают ее всего лишь отдельным штрихом общей нерадостной картины, нарастающей глобальной тенденции тотального безразличия наемных работников к интеллектуальной собственности работодателей, к наносимому ими ущербу компаниям ради собственной выгоды.

Рецензии

Fraud Analytics: Strategies and Methods for Detection and Prevention
By Delena D. Spann; reviewed by James E. Sellers, CPP
John Wiley & Sons, Inc.; wiley.com; 176 pages; $50.

Книга представляет собой отличное пособие для расследователей мошенничества на предприятиях. Она знакомит с широким инструментарием расследований. Не перегружена техническими терминами, читается легко и понятно, даже теми, у кого английский язык не родной.

Конкретные примеры (case studies) подкрепляют аналитический подход к теме, демонстрируют практическое применение инструментов расследований.

Книга особенно рекомендуется всем, кто занимается финансовыми расследованиями, и может быть включена как учебное пособие в соответствующие дисциплины и курсы.

Practical Aviation Security: Predicting and Preventing Further Threats, Second Edition
By Jeffrey C. Price and Jeffrey S. Forrest; Reviewed by Paul Stanley, CPP
Butterworth-Heinemann. Available from ASIS, item #2067; 500 pages; $80 (ASIS member), $88 (nonmember)

Это уже второе издание.

Авторы подчеркивают, что терроризм – далеко не единственная угроза безопасности в авиации. Они публикуют перечень преступлений, совершаемых в аэропортах, от вандализма до сбыта наркотиков и нелегального оружия.

Книгу отличает глубина исследования, которое охватывает факты из жизни, вопросы права, анализ конкретных ситуаций. Книга полезна всем, кто, так или иначе, связан с вопросами обеспечения безопасности в гражданской авиации, включая все уровни контроля и проверки, начиная с момента попадания пассажира в здание аэропорта.

Рецензии

Fraud Analytics: Strategies and Methods for Detection and Prevention
By Delena D. Spann; reviewed by James E. Sellers, CPP
John Wiley & Sons, Inc.; wiley.com; 176 pages; $50.

Книга представляет собой отличное пособие для расследователей мошенничества на предприятиях. Она знакомит с широким инструментарием расследований. Не перегружена техническими терминами, читается легко и понятно, даже теми, у кого английский язык не родной.

Конкретные примеры (case studies) подкрепляют аналитический подход к теме, демонстрируют практическое применение инструментов расследований.

Книга особенно рекомендуется всем, кто занимается финансовыми расследованиями, и может быть включена как учебное пособие в соответствующие дисциплины и курсы.

Practical Aviation Security: Predicting and Preventing Further Threats, Second Edition
By Jeffrey C. Price and Jeffrey S. Forrest; Reviewed by Paul Stanley, CPP
Butterworth-Heinemann. Available from ASIS, item #2067; 500 pages; $80 (ASIS member), $88 (nonmember)

Это уже второе издание.

Авторы подчеркивают, что терроризм – далеко не единственная угроза безопасности в авиации. Они публикуют перечень преступлений, совершаемых в аэропортах, от вандализма до сбыта наркотиков и нелегального оружия.

Книгу отличает глубина исследования, которое охватывает факты из жизни, вопросы права, анализ конкретных ситуаций. Книга полезна всем, кто, так или иначе, связан с вопросами обеспечения безопасности в гражданской авиации, включая все уровни контроля и проверки, начиная с момента попадания пассажира в здание аэропорта.

Использование оружия в охране больниц

Проведенный Медицинским центром при Duke University опрос ставил задачей

исследовать методы предупреждения и прекращения насилия в учреждениях здравоохранения, включая вопросы использования охраной разных видов оружия.

Опрос проводился среди членов международной ассоциации охранных структур в сфере здравоохранения (Association of Healthcare Security and Safety), но только работающих в США. На опрос откликнулись 299 респондентов. Большинство из них – руководители охранных структур, 62% с опытом работы в этой области более 10 лет.

Вот некоторые выводы.

87% госпиталей организуют для всех охранников специальные тренинги, связанные с фактами насилия. Для медперсонала такие тренинги осуществляют 64% больниц, для административного состава – 28%, для работников пищеблока – 27%, для техников – 4%. Только 14% госпиталей практикуют обучение всего персонала.

Металлодетекторы используют 33% госпиталей. Это, как правило, крупные медицинские центры. Обычно такое оборудование монтируется у дверей, ведущих в подразделение скорой помощи. Оборудование, установленное при главном, общем входе в здание, встречается редко, что объясняется желанием администрации не травмировать посетителей строгим контролем.

Что касается технического оснащения и вооружения охранников, то практически везде (96%) используются наручники, меньше – полицейская дубинка (56%), травматическое оружие – 52%, огнестрельное оружие (пистолет) – 52%, электрошокеры TASERS – 47%, сторожевые собаки – 12%.

90% госпиталей практикуют регулярные занятия по владению и использованию оружия. Примечательно, что наиболее эффективным исследователи находят электрошокеры. Там, где они на вооружении, количество случаев насилия меньше на 40%, чем там, где их не используют.

Факты применения насилия более всего связаны с поведением пациентов (75%), а также посетителей (9%). Обычно дело ограничивается угрозами и бранью (41%), физическое насилие фиксируется в 29% конфликтов.

В течение последнего года практический каждый медицинский центр сталкивался с фактами насилия внутри учреждения, в среднем 123 случая на одну больницу.