Охрана предприятия

№1 (35), 2014

Оглавление

США: дефицит кадров в сфере информационной защиты

Книжное обозрение

The Safe Hiring Manual: The Complete Guide to Employment Screening Background Checks

Исследования

Экономический кризис и кражи в розничных сетях

Национальные различия и общее в подходе к приоритетам безопасности

Журнал Security Magazine опубликовал результаты представительного опроса более 200 крупнейших компаний в США, Великобритании, Дании и Швеции относительно работы корпоративных служб безопасности.

Анализ ответов выявил серьезные расхождения в понимании взаимодействия между государством и бизнесом в вопросах противодействия терроризму, но в то же время подчеркнул схожесть позиций по вопросам профессионализма и новых тенденций в приоритетах безопасности.

За последнее десятилетие, отмечает журнал, значение корпоративной безопасности стремительно выросло. Соответственно возрос авторитет и статус руководителя СБ. Такая тенденция особенно характерна для США, где за последние годы появилось множество учебных программ, раздвигающих границы знаний в области технологий безопасности, защиты информации, анализа и управления рисками.

Другая важная тенденция – охрана предприятия становится важным компонентом, неразрывной частью бизнес стратегии. Если ранее доминировал узкий подход к безопасности как отдельно стоящей функции физической охраны персонала и имущества, то сегодня на СБ возлагаются более широкие задачи, включающие анализ и управление рисками, защиту информации и противодействие терроризму. В таком подходе едины практически все офицеры безопасности, независимо от того, в какой стране они живут и работают (в рамках данного исследования речь идет о четырех государствах).

Отвечая на вопрос, какие наиболее важные шаги были сделаны для повышения эффективности их работы, директора СБ практически единодушно указали на:

- «сбор развединформации об угрозах компании»,
- «усиление и модернизация СКУД»,
- «внимание к управлению в чрезвычайной ситуации» (emergency management).

Если контроль и управление доступом в числе приоритетов не вызывает удивления, то выдвижение разведки на верхнюю строчку приоритетов – нечто новое для отрасли индустрии. Очевидно, такая тенденция обусловлена растущей нестабильностью бизнес среды. Сегодня все чаще разведка воспринимается как центральное условие продуктивного анализа рисков и планирования для форс-мажорных ситуаций.

В чем замечены серьезные расхождения, так это в отношении контртерроризма. В ответах на вопрос о роли государства и бизнеса в деле противодействия терроризму офицеры по безопасности в США и Англии в подавляющем большинстве выразили несогласие с той точкой зрения, что такие задачи ложатся преимущественно на государство. Они уверены, что здесь ведущая роль принадлежит тесному партнерству между государством и бизнесом. В то же время в Дании и Швеции большинство считает, что борьба с терроризмом – задача главным образом государства, в последнюю очередь – бизнес организаций.

Такие расхождения вполне объяснимы. В США и Великобритании компании охотнее идут на сотрудничество с правительственными спецслужбами (в США – 67% компаний, в Великобритании 65%, Швеции 49%, в Дании только 18%). Другое объяснение лежит в плоскости исторической роли государства в экономической и общественной жизни. В Швеции и Дании государство традиционно более влиятельно и сильно, чем во многих других странах, поэтому тамошние бизнесмены в вопросах борьбы с терроризмом склонны возлагать надежды на правительственные структуры.

Главные технологии и инновации в сфере безопасности в 2014 году

Группа экспертов технологической компании Sogeti сформулировала определяющие для 2014 года, по их мнению, тенденции в области технологий безопасности:

Мобильность – везде, в любое время, любых девайсов

Сегодня мобильность средств коммуникации прямо влияет на производительность труда пользователей, независимо от того, кому принадлежат мобильные носители информации – организации или служащим. Отсюда – все более острая проблема обеспечения безопасности коммуникаций через мобильные устройства как внутри организации, так и с внешними корреспондентами, повышенное внимание к формулированию и соблюдению соответствующих корпоративных политик.

Укрупненная реальность

«Укрупненная реальность» (Augmented Reality) – видение, прямое или опосредствованное, реального, физического мира, элементы которого укрупняются с помощью звука, видео, графики, GPS данных, что имеет важное значение для изучения бизнес среды.

Большие Данные

Под термином «Большие Данные» подразумевается новое поколение технологий, предназначенных для быстрого поиска, извлечения ценной информации из океана

данных, ее анализа. Такие технологии необходимы для своевременного обнаружения рисков и угроз.

Облачные исчисления

Ожидается, что в 2014 году буду возникать новые облачные технологии, например, позволяющие интегрировать информационные услуги из различных источников в едином приложении. Все большее применение будут находить облачные исчисления в развитии и использовании мобильных девайсов.

Информатизация сферы корпоративной безопасности

Охрана предприятия будет во все большей степени опираться на информационные технологии, не полагаясь исключительно или преимущественно на охрану периметра. Более сбалансированный и эффективный подход к исследованию угроз и рисков будет обеспечиваться с помощью облачных сервисов, мобильных устройств, веб технологий, что в свою очередь потребует новых программных решений, заточенных на проблемы охраны и безопасности.

Снижение себестоимости за счет повышения качества

Звучит шаблонно, но, как свидетельствуют эксперты, этот аспект нередко игнорируется. Сегодня вопросы качества напрямую соотносятся с проблемами эффективной охраны предприятия. Проверка (тестирование) качества продукции перестает быть делом одних лишь технологов, но требует комплексного подхода, участия всех звеньев предприятия, включая и службу безопасности.

Печать 3D

2013 год стал поворотным в овладении технологией печати в формате 3D. 3D принтеры проявили способность производить продукты из разных материалов (пластика, металлов, т.д.), что обусловливает новые проблемы с точки зрения безопасности. Так, в частности, в США обеспокоены перспективой нелегального производства из пластики с помощью этих технологий огнестрельного оружия, которое, к тому же, в отличие от металлических изделий трудно сканировать при проверке в аэропортах и иных общественных объектах.

Интернет вещей

Концепция «Интернета Вещей» предполагает реальные сегодня возможности на расстоянии управлять сенсорными данными, дистанционно контролировать физические объекты. Это позволяет по-новому взглянуть на нашу повседневную активность, на производство и бизнес процессы, включая управление рисками.

(по материалам журнала Security Magazine)

Контрразведка в охране предприятия

На страницах онлайнового журнала Scip.insight, посвященного вопросам конкурентной разведки, глава компании Aurora WDC Дерек Джонсон рассказывает о том, как

программа контрразведки, осуществляемая силами корпоративной службы КР (конкурентной разведки), помогает в охране интеллектуальной собственности предприятия.

Эффективная программа контрразведки, пишет автор, исходит из необходимости донесения до каждого сотрудника четких инструкций относительного того, что можно, а что нельзя разглашать публично относительной своей компании. В руководящем эшелоне, как правило, хорошо об этом осведомлены и следуют правилам сохранения коммерческой тайны. Угрозы возникают в среднем и низшем звеньях менеджмента. Те, кто работает «на передовой» - продавцы, специалисты по маркетингу, развитию продукта, на технологическом, инновационном направлениях, - то есть хорошо информированные о делах своей организации профессионалы, являются главным объектом конкурентной разведки, а то и промышленного шпионажа. Именно на них в первую очередь ориентируется работа контрразведки.

Такие программы можно сегодня встретить во многих западных компаниях независимо от их бизнеса и размера. При этом важно отметить, что зачастую эти программы формируются и осуществляются профессионалами конкурентной разведки. И это не случайно. Автор, например, настаивает, чтобы профессионалы КР участвовали в информационной защите предприятия, так как они, может быть, лучше других осведомлены о путях и методах сбора конкурентной информации, в том числе и не всегда легальными и этическими способами.

Дерек Джонсон рекомендует регулярно, не реже одного раза в год, проводить тестирование систем защиты интеллектуальной собственности для выявления и последующего устранения уязвимостей. Это сложная операция, которая в зависимости от размера организации занимает от 2 до 4 недель.

По ее завершении подбиваются итоги. С персоналом проводятся учебные и тренинговые занятия, охватывающие всю структуру организации – от ведущих разработчиков новых технологий до вспомогательного персонала (уборщиков, шоферов и т.п.). Для новичков, принимаемых на критически важные позиции в организации (продажи, исследование и развитие продукта), такие занятия могут длиться от 2 до 5 дней.

Автор рекомендует через полгода, самое большее – год, проводить повторное тестирование с упором на те звенья, которые в ходе последнего тестирования заявили о себе как наиболее слабые, уязвимые.

Дерек Джонсон излагает предполагаемый сценарий в случае игнорирования контрразведки. Компания А вышла на рынок с инновационным продуктом, который обещает прибыль в 10 миллионов долларов за первые 12 месяцев продаж. Однако конкурент Б не дремал и использовал инструментарий конкурентной разведки для сбора информации, на основе которой начал разработку собственной альтернативы. Если ему удается выпустить свой продукт к концу десятого месяца продаж компании А, то, как нетрудно подсчитать, последняя теряет 1.67 миллионов долларов. Чем раньше конкурент подсуетится, тем больше упущенная выгода.

Конечно, создание и осуществление программы контрразведки требует вложений, которые зависят от амбициозности проекта и размеров организации. Но эти затраты с лихвой окупаются, если программа надежно защищает интеллектуальную собственность организации от поползновений конкурентов.

Большие Данные и СКУД

Одна из проблем, связанных с обеспечением безопасности массовых, в том числе спортивных, мероприятий, заключается в том, что зачастую невозможно заранее определить, кто из посетителей потенциально опасен. Продажа билетов, как правило, осуществляется все еще анонимно. Конечно, кое-где вводится система интернет продаж по удостоверениям личности, но нет гарантии, что купленный билет не попадет в другие руки.

Решение проблемы автор публикации в журнале Security Magazine (December 1, 2013) Стив Ван Тилл видит в возрастающей тенденции использовать мобильные девайсы, прежде всего сматфоны, для приобретения билетов в театры, в кино, на стадионы…Современные смартфоны обладают функциями удостоверения (верификации) личности владельца и GEO отслеживания (geo-tracking) посредством GPS.

Но какое отношение все это имеет к Большим Данным? Самое прямое, утверждает автор заметки. Огромный массив данных, которые проходят через мобильные устройства, невозможно контролировать традиционными инструментами аналитики, особенно в реальном времени. Но задействовав современные программные средства сбора и анализа информации, можно с довольно высокой степенью надежности проследить, кто пришел на массовое мероприятие.

В индустрии безопасности давно идут дискуссии на тему, как использовать данные корпоративной безопасности для повышения доходности компаний и организаций. Прямую связь здесь установить зачастую нелегко. Но на примере выше мы видим, что технологии, связанные с мобильными девайсами, позволяют собирать, анализировать статистические данные: кто посещает эти мероприятия, как часто, в какое время приходит, когда уходит, когда уходит и возвращается, и т.д. А такая обработанная информация уже имеет прямое отношение к бизнес планированию, к маркетингу, рекламе и прочим коммерческим аспектам деятельности организации.

Еще одна сфера, где работа с Большим Данными способна приносить ощутимую пользу – управление коммерческой недвижимостью. Владельцы зданий нередко имеют смутное представление, кто, когда и как часто приходит к арендаторам. В некоторых случаях вход свободный. В других - выставлена охрана, которая самое большое, что может делать, это проверять и выписывать пропуска. Как и в случае приобретения билетов, использование мобильных устройств для доступа в охраняемые помещения дает огромный массив данных, представляющих ценность не только для службы безопасности, но и для бизнеса.

В больших зданиях посетители обычно делятся на две большие группы: персонал компаний-арендаторов и гости. Традиционные системы выписки пропусков, проверки удостоверений личности, сканирования приносимых вещей не способны обеспечивать надлежащий сбор статистики, имеющей коммерческое значение. Это возможно с использованием мобильных девайсов, которые не только облегчают охранникам проверку посетителей, но и позволяют в автоматическом режиме собирать и обрабатывать коммерчески нужную информацию.

Видеонаблюдение против магазинных краж

Опрос 125 розничных компаний в США выявил рост магазинных краж. 96% опрошенных заявили о кражах в 2013 году (94.5% в 2012 году) (securitymanagement.com).

Один из путей успешной борьбы с этим злом, полагают эксперты, - налаживание сбора правдивой информации о клиентах. До недавнего времени ритейлеры в штате Техас были лишены такой возможности, отмечает журнал Security Management/ Этот штат был одним из двух, где законодательство запрещало хранить в электронном виде информацию, сканированную с удостоверений личности (водительских прав). Между тем, потери от воровства в магазинах Техаса достигали ежегодно миллиарда долларов!

Наиболее привлекательны для криминала фармацевтика и ювелирные изделия. Охотники за наркотическими препаратами и драгоценностями совершенствуют свое ремесло, изобретают новые приемы. В этом им помогает интернет, где преступники совершенно свободно обсуждают пути и способы нелегального обогащения. За последние годы получил распространение способ, при котором злоумышленники не взламывают двери и окна. Они просто проникают внутрь помещения через проделанное в крыше отверстие, отключают тревожную сигнализацию, ломают видеокамеры. В отдельных случаях позволяют сработать сигнализации, прибывший наряд полиции находит двери и окна не взломанными и уезжает, и это повторяется несколько раз, пока полиция не перестает обращать внимание на «неисправную» систему (или отключает ее до утреннего ремонта). Кроме того, сокращение числа полицейских из-за кризиса также играет на руку криминалу: в крупных городах полиция физически не может реагировать на каждый поступающий в участок сигнал.

В этой связи полиция все меньше полагается на традиционные тревожные сигнализации, которые нередко грешат ложными вызовами, акцент делает на технологии, где беспроводные сенсоры, интегрированные с видеонаблюдением, позволяют обнаружить вора, снимать картинку и одновременно посылать видео сигнал в полицейский участок, на экран монитора. Там, где появилась эта технология, заявляют в полиции, количество задержаний выросло на 50%.

Совсем недавно под давлением бизнеса в штате Техас все же принят закон, разрешающий предпринимателями сканировать и хранить в электронном формате информацию водительских прав, что усиливает их позиции в противодействии преступникам. Сегодня цифровые технологии видеонаблюдения активно осваиваются владельцами магазинов и розничных сетей. Причем не только для борьбы с воровством. Статистика, собираемая рекордерами, позволяет изучать, у каких прилавков собирается больше всего покупателей, насколько внутренняя планировка отвечает потокам клиентов, какова демография посетителей, где должны концентрироваться продавцы в разное время работы и т.п. Кроме того, видеонаблюдение предполагает контроль за ситуацией в магазине дистанционно.

Системы сигнализации и массового оповещения в учебных заведениях

Эрик Колман, руководитель службы безопасности Texas A&M University, установил тревожные телефоны (emergency phones) по всей территории кампуса – вдоль пешеходных дорожек, на паркинге, у всех входов и выходов и даже в каждой аудитории. Это означает, что студенту, где бы он ни находился, требуется всего несколько шагов, чтобы позвать на помощь. Как только он снимает трубку, сигнал поступает на пульт диспетчера, который сразу же определяет месторасположение пункта связи и далее передает информацию офицерам безопасности. Более того, каждый узел тревожной связи снабжен камерой видеонаблюдения, что позволяет осуществлять мониторинг территории и помещений университета 24 часа в сутки в режиме реального времени.

В Университете Буффало особое внимание уделяют системе массового оповещения, которая охватывает 11 000 студентов, давших согласие на включение в данную систему. Сообщения приходят на личные мобильники. Также предусмотрено использование социальных сетей.

Служба безопасности университета Northen Kentucky технологию массового оповещения интегрировала с системой СКУД, где каждый пост представляет собой антивандальное, беспроводное, маломощное, но высоко эффективное устройство. Программа позволяет наглухо запереть двери в одном, нескольких избранных помещениях или везде одновременно.

Многие школы в США для обеспечения безопасности учащихся выбрали и используют беспроводную систему тревожной кнопки. Каждый преподаватель, инструктор имеет при себе т.н. «бэджик безопасности» на основе технологии RFID (радиочастотная идентификация). В случае опасности нажатием кнопки посылается сигнал тревоги, который автоматически определяет местонахождение обладателя устройства. Преимущества такой системы перед проводными стационарными средствами тревожной сигнализации очевидны. Программа позволяет использовать мобильные устройства тревожной сигнализации также и для массового оповещения об угрозах и опасностях.

Технология Wi-Fi сегодня востребована практически во всех колледжах и университетах Америки. Она также может служить задаче массового оповещения и предупреждения об опасности. Это видно на примере University of New Hampshire, администрация которого обеспечила свободный Wi-Fi для тысяч участников и зрителей массовых мероприятий в принадлежащем университету спортивно-развлекательном центре. За последний год центр посетили четверть миллиона человек. Задача ставилась не только предоставить посетителям возможность пользоваться Интернетом для переписки, скачивания фото и видео материалов, но и для распространения по локальной интернет сети (университета) сообщений информационного характера и разного рода оповещений.

(по материалам журнала Security Magazine)

Расходы на охрану предприятия отстают от возрастающих с каждым годом угроз

Исследование, проведенное осенью 2013 года компанией PricewaterhouseCoopers и онлайновым журналом Chief Security Officer, показало, что хотя многие организации из года в год увеличивают вложения в охрану предприятия, в частности, в информационную защиту, денег на успешную борьбу с растущим числом угроз со стороны криминала критически не хватает. Преступность не стоит на месте, постоянно совершенствуется, изобретая все новые способы и методы своей деятельности. Средний по кампаниям ущерб от преступлений растет ежегодно на 20 с лишним процентов. Основной вывод: внедрение технологий безопасности не поспевает за увеличивающимися и все более изощренными угрозами.

Одна из причин отставания, полагает Майк Ротман, президент исследовательской фирмы Securosis, заключается в разобщенности бизнес менеджеров и специалистов по безопасности, включая профессионалов в отделе информационных технологий. В ряде компаний специалист по информационной защите просто теряется где-то внизу корпоративной иерархии, хотя по своей должности он должен напрямую выходить на вице-президента, докладывать о проблемах первым лицам. Кроме того, выбор и закупка нового информационно-технологического оборудования нередко проходит без участия и консультации с экспертами по физической охране и защите информации.

Другая причина отставания имеет прямое отношение к модным сегодня облачным исчислениям. Ими сегодня пользуются почти половина американских компаний, но только каждая пятая из них включает правила безопасности работы «в облаках» в свои корпоративные политики и инструкции.

Существует и такая проблема: крупная компания переводит в «облака» значительную часть систем и функций, но ее мелкие поставщики, партнеры, фирмы-клиенты не пользуются в силу разных причин серьезными информационными технологиями и не испытывают необходимости переходить на облачные исчисления. Это различие создает определенные риски, когда партнерские отношения подразумевают обмен информацией, базами данных.

Средств на охрану предприятия не хватает и по той простой причине, что растет стоимость технологий безопасности, равно как и их эксплуатации. Некоторые эксперты уверены, что организации ошибаются, когда при выборе средств защиты упор делают на дорогостоящие технологии предупреждения кибератак, пренебрегая методологией быстро и эффективно реагировать на фактически осуществленные несанкционированные проникновения и взломы сетей. Многие организации так и не научились их своевременно обнаруживать и адекватно реагировать. Успешные хакерские атаки остаются незамеченными, либо обнаруживаются слишком поздно. Только чуть больше половины американских компаний практикуют постоянный мониторинг сетевого трафика. Еще меньше организаций используют специальные системы управления данными и контроля безопасности в сетях для выявления инцидентов.

Даже в тех компаниях, которые не жалеют средств для внедрения технологий, позволяющих эффективно обнаруживать и отвечать на кибератаки, зачастую просто нет собственных профессионалов, которые могут самостоятельно, без приглашения специалистов извне, управлять новой сложной техникой.

Взаимодействие между службами безопасности и информационных технологий – не решенная проблема

Для многих организаций координация работы офицеров безопасности и ИТ профессионалов остается неразрешимой проблемой, пишет Стэси Коллетт в онлайновом журнале Chief Security Officer. Отсутствие взаимопонимания, а то и взаимное недоверие, соперничество и ревность между этими службами негативно влияют на безопасность компаний.

Одни занимаются физической охраной, другие – защитой сетей и информации. Но есть зоны и вопросы, настоятельно требующие совместных, слаженных усилий. И вот здесь нередко возникают разногласия, если не конфликты. В статье описывается такой пример из реальной действительности. Вице-президент средней по размеру компании на юго-западе США потребовал установить в рецепции новые, более совершенные камеры наблюдения, после того, как действующие видеокамеры оказались не в состоянии зафиксировать и сохранить данные о несанкционированном проникновении в помещения компании. Сотрудники отдела ИТ, полагая, что видеонаблюдение является исключительно их сферой полномочий, установили веб-камеру, включать которую пришлось бы рецепционисту вручную каждый раз при возникновения инцидента безопасности. «Эти ребята из отдела информационных технологий ни черта не понимают в вопросах охраны предприятия, - комментировал позднее вице-президент, - конечно, видеооборудование необходимо для безопасности, но все, что касается физической и персональной охраны – не их ума дело».

Часто говорят о необходимости интеграции и конвергенции в сфере охраны предприятия, замечает автор статьи, но на деле многие предприниматели считают конвергенцию несбыточной мечтой, поскольку подавляющее большинство офицеров безопасности совершенно беспомощно в технических вопросах.

В последние несколько лет отчетливо наблюдается существенный рост спроса на универсально образованных офицеров безопасности, обладающих широкими познаниями, включая технические, технологические аспекты безопасности. Но пока это дело будущего, а сегодня многие организации нуждаются в налаживании тесного сотрудничества технарей и охранников.

Соперничество, взаимное недоверие нередко обусловлены неправильным толкованием понятия «безопасность», использованием не одних и тех же терминов, считает Тим Уильямс, директор безопасности Caterpillar Inc. Если в названии должностей, в определении служебных полномочий заменить слова «охрана», «безопасность» на термины «риски», «угрозы», то обеим сторонам легче прийти к взаимопониманию, проще наладить совместную работу.

Людей сплачивает необходимость решать общую задачу, подчеркивает Крис Никерсон, основатель фирмы Lares Consulting, которую приглашают для моделирования и проведения тестовых атак на системы физической и информационной защиты. В ходе одной из таких проверок Никерсону удалось воспользоваться ротозейством сотрудника, овладеть на его личной страничке в LinkedIn служебным паролем, проникнуть в программу СКУД, украсть код электронного пропуска и в конечном итоге беспрепятственно пройти в тщательно охраняемое помещение компании-клиента. Этот пример наглядно показывает, что у технарей и охранников общая задача: «остановить злоумышленника».

Как планировать первые, «золотые», минуты после инцидента

Об этом аспекте планирования действий в чрезвычайной ситуации (авария, стихийное бедствие, террористическая угроза и т.п.) идет речь в публикации на сайте securitymagazine.com, November 5, 2013).

Координация с местными властями в случае возникновения форс-мажорной ситуации занимает важное место в планах. Однако в первые, «золотые», минуты после инцидента, пока не поспела помощь извне, на происшествие реагируют работники организации: спасают имущество, отключают электрооборудование, обеспечивают эвакуацию, решают прочие задачи. Обычно в планах безопасности четко расписано, кто и за что конкретно отвечает. Но планы планами, а люди в своей повседневной работе зачастую имеют весьма смутное представление, что они должны делать в реальной форс-мажорной ситуации. Но именно от слаженных действий каждого и коллектива в целом во многом зависит размер ущерба, тяжесть последствий инцидента.

Существует справедливое мнение, что в минуту кризиса люди паникуют и делают непоправимые ошибки. Это происходит тогда, когда они не имеют достоверной информации, в результате чего:

- игнорируют происходящее

- ждут подсказки руководства.

- спешат на место происшествия, чтобы узнать, что случилось.

- делают то, что им привычнее, например, устремляются к основному, главному выходу, игнорируя запасные лестницы и двери, создавая толкотню, пробки.

Напротив, как показывают исследования, их поведение адекватно ситуации, если они:

- имеют ясное представление о том, что произошло.

- четко знают, как поступать и что делать в сложившейся обстановке.

Как донести необходимую информацию? Важную роль играют специальные тренинги. Но работники компании не солдаты, которые каждодневно готовят себя к ратным

делам. Поэтому первостепенное значение приобретают средства коммуникации, с помощью которых персонал информируется, действия людей координируются и направляются. Используются все доступные и возможные виды связи. Сообщения повторяются, дублируются, корректируются соответственно меняющейся ситуации.

Современные коммуникационные технологии позволяют не ограничиваться подачей тревожной сирены, но моментально распространять инструкции и распоряжения. Целесообразно заранее записать варианты голосовых сообщений на разные случаи. При этом важно учитывать ряд обстоятельств.

Локализация. Если инцидент затрагивает только часть организации (скажем, одно из нескольких зданий предприятия), то текст сообщений варьируется в зависимости от адресата. Тем, кто оказался в опасной зоне, подсказываются пути и способы спасения. Остальным – рекомендация не приближаться к опасному участку.

Автоматизация. Современные технологии позволяют без вмешательства людей начать массовое оповещение, как только сенсорные устройства включают режим тревоги.

Мобильность. Мобильные устройства дают возможность быстрого распространения информации с любого места в организации или извне.

Интеграция. Некоторые программные продукты предполагают возможность одновременного использования разных средств коммуникации – сирен, проблесковых маячков, голосовых инструкций, тестовых сообщений на мобильники и компьютеры.

Автономное энергопитание. В планах надо учитывать опасность отключения электроэнергии (например, в случае крупного стихийного бедствия). Чтобы обеспечить работу компьютеров и сотовых телефонов, заранее предусмотреть запасные источники электропитания (генераторы, аккумуляторы).

Ваш не столь уж «умный» дом

С этим названием на сайте csoonline.com в конце 2013 года опубликован материал Тейлора Армединга. Автор заметки предупреждает об опасностях и рисках, которые могут возникать при использовании модных ныне дистанционных систем управления домашним хозяйством.

Конечно, такие технологии создают удобства. Вы можете убавить или прибавить температуру отопления, находясь за тысячи миль от своей квартиры, закрыть или открыть гаражные ворота и т.п…Вместе с тем, нельзя забывать, что новые технологии «умного дома» несут огромные риски. Хорошо подготовленный хакер может без особого труда взять под контроль систему дистанционного управления, отключить тревожную сигнализацию, отпереть двери, внести изменения в режим работы отопления или холодильной установки, создать массу других проблем.

Эксперты из компании Trustwave SpiderLabs продемонстрировали журналистам легкость, с которой хакеры могут взламывать популярную в Америке систему автоматических (гаражных) ворот VeralLite, которую выпускает фирма Mi Casa Verde. Уязвимость этой системы заключается в том, что для срабатывания не требуется ни

пароля, ни имени владельца. Доступ хакера к вашей домашней интернет сети означает доступ к вашему дому.

Кроме VeralLite эксперты испытали десяток других аналогичных продуктов и только два из них не удалось взломать. Большинство продающихся на рынке систем управления домом не имеют сколько-нибудь серьезной защиты. Газета «Нью-Йорк таймс», комментируя результаты испытаний, пришла к выводу, что нельзя верить ни одной компании, которая заявляет, что их продукция надежно, гарантированно защищена от хакеров.

Кевин Митник, в прошлом известный хакер, а сегодня респектабельный владелец компании Mitnick Security Consulting, говорит, что о рисках таких систем было известно всегда, но сегодня интерес к использованию технологий «умного дома» растет с каждым днем и, как правило, эти системы работают через Интернет. По его словам, проблема в том, что они имеют очень слабое отношение к безопасности дома, и пользователям приходится в этом вопросе полагаться исключительно на производителя. Специалист заявил, что он ни за что не стал бы приобретать систему с интернет технологией, которую бы он сам смог вскрыть.

Эксперт Рожер Торнтон, главный технический директор Alien Vault, согласен, что данные системы имеют массу уязвимостей, но, вместе с тем, уверен, что вопросы защиты находятся в компетенции самих пользователей. «Если вы не в состоянии создать и настроить частную виртуальную сеть (virtual private network) и управлять операциями по ее защите, то лучше дважды подумать, стоит ли вам приобретать систему «умного дома». Любая из них может быть взломана хакерами или спецслужбами. В отличие от компьютеров такие системы часто невозможно переделать, улучшить, дополнить новыми функциями. И если хоть раз она успешно взломана, то будет подвергаться атакам неоднократно на всем протяжении ее эксплуатации.

Совет бывшего хакера потребителям: «Не подключайте свое жилище к Интернету, если не имеете элементарных навыков и опыта в вопросах мониторинга и защиты сети. В принципе это дело не сложное. Большинство людей, сами или с помощью толковых детей, могут создать и управлять мини сетью с применением программных решений, которые используются сегодня в компаниях, но с каждым днем становятся все проще, дешевле, доступнее».

От металлических ключей к электронным картам

Первые в истории известные нам ключи использовались египтянами 4 000 лет тому назад. Тогда они представляли собой деревянную втулку с зубцами. Металлические ключи появились в Европе позднее. Древние римляне впервые применили выступы и выемки в бородке ключа и замке – технологию, которая дожила до наших дней.

Когда в американском городе Crown Point местный суд переехал в специально выстроенный для него комплекс, то прежнее трехэтажное старинное здание переоборудовали под офисную аренду, не меняя замки и ключи. Вот здесь то и

начались проблемы. К арендаторам (разным компаниям и фирмам) пошел густой поток посетителей, уследить за которыми служба безопасности не в состоянии. Фонд, владеющий зданием, принял решение взять на вооружение систему электронного дистанционного контроля. Новая СКУД адаптирована под особенности здания: два входа их четырех ведут на первый этаж, где разместились магазины, а остальные – на второй и третий этажи, где кроме офисов, устроен танцевальный зал. При этом программа СКУД настроена таким образом, что оставляет открытым вход в танцевальный зал по вечерам и в выходные, держа на запоре офисные помещения. С учетом культурно-исторической ценности здания, использованы беспроводные технологии контроля и управления доступом.

В университете Auburn используется СКУД на основе уникальной технологии распознавания радужной оболочки глаза. Все обладающие доступом смотрят в камеру на достаточно коротком расстоянии, но без необходимости вытягивать голову непосредственно к глазку. Процесс идентификации занимает менее секунды. Система пропускает 12 человек в минуту. Она безошибочно работает, даже если посетитель носит очки (включая солнцезащитные) или линзы. Удобство данной технологии в том, что она не требует от студентов иметь при себе электронные пропуска, которые они часто теряют.

А в университете Майями, где установлена электронная пропускная система с картами и считывателями, студент, забывший или потерявший пропуск, посылает со своего мобильника в программу СКУД текст с условными словами, на которые система срабатывает, открывая дверь. Переход от обычных металлических ключей к электронным позволяет экономить в год десятки тысяч долларов, которые, в частности, тратились на замену сломанных или потерянных ключей.

Программные технологии не в новинку во многих американских школах. Ими охотно пользуются в 114 школах округа Cobb, штат Джорджия. Для начала там провели пилотный проект в одной из начальных школ, где установили систему считывателей электронных карт и автоматических дверных задвижек (щеколд). Системой СКУД охвачены все входные двери, ворота для въезда школьного автобуса, даже вход на спортивную площадку. Вскоре такая система заработала во всех учебных заведениях округа. При этом деревянные двери, там, где они были, пришлось заменить металлическими. Плюс ко всему в СКУД встроена программа мониторинга, которая автоматически проверяет, все ли двери заперты на засов. При обнаружении, что какая-то дверь открыта или задвижка не сработала, в администрацию школы идет автоматический запрос. Если в течение 15 минут ответа нет, то сигнал тревоги передается в ближайший участок полиции.

(по материалам веб-сайта securitymagazine.com)

Как обеспечить безопасность и защиту информации на собраниях акционеров

Свои рекомендации предлагает Гарлан Кэлхоун, вице-президент Alliedbarton Security Services. Материал опубликован 2 декабря 2013 года на сайте csoonline.com.

Автор начинает со статистики. Кража интеллектуальной собственности стоит американским компаниями порядка 1 миллиарда долларов в год. На собраниях акционеров нередко обсуждаются такие чувствительные вопросы как ценовая политика, маркетинговые и рекламные стратегии, зарплаты персонала, правовые аспекты бизнеса. Задача службы безопасности – обеспечить, чтобы эта и иная конфиденциальная информация не попала в распоряжение конкурентов.

Не позднее, чем за три месяца до собрания все заинтересованные службы и управления, включая кадровиков и юристов, начинают процесс планирования. Надо сформулировать и ответить на ряд существенных вопросов: Как много людей ожидается на собрании? Где будет происходить мероприятие – на территории компании или вне ее? Выбор нейтрального помещения (т.е. за пределами предприятия) потребует больше усилий и средств защиты. Достаточно ли своих сил для обеспечения надежной безопасности? И так далее.

Планирование включает также мониторинг социальных сетей и новостных лент по данной отрасли экономики с целью понять, на чем фокусируется внимание общественности и экспертов. К примеру, если речь идет о компании по добыче шельфовой нефти, то вопрос: как ее деятельность оценивается такими организациями как Гринпис?

За месяц по собрания проводится сценарный анализ, где проигрываются кризисные ситуации и инциденты. К примеру, кому-то из участников собрания плохо с сердцем. Или не в меру агрессивно ведет себя участник собрания. Или внезапно погас свет…..

За день или накануне мероприятия помещение, где проводится мероприятие, тщательно проверяется на наличие «жучков». На входе в зал устанавливается металлический детектор. Желательно, чтобы смартфоны, компьютеры, видео и аудио записывающие устройства у всех участников отбирались и хранились в специальной комнате. Исключение – только для тех выступающих, кто использует средства визуальной презентации. При этом допускается одно для всех докладчиков компьютерное устройство, которое также тщательно проверяется.

Всех участников заранее предупреждают о необходимости проявлять осторожность в работе с письменными документами. Бывает, что важные бумаги по забывчивости оставляют в фойе, в баре, других общественных местах.

Особое внимание надо уделить поведению миноритарных акционеров, которые, случается, ведут себя некорректно, агрессивно. Поэтому протокол безопасности, который доводится до сведения всех участников, должен содержать меры по обузданию таких акционеров, вплоть до удаления из зала заседания. То же самое относится и к особо наглым журналистам.

Следует иметь план действий в экстремальных условиях, например, когда необходимо всех срочно эвакуировать (при сигнале о заложенной бомбе) или вызвать скорую помощь.

С обслуживающим персоналом (скажем, техническим персоналом отеля) надо подписать соглашения о неразглашении информации, получаемой ими во время работы на мероприятии.

После завершения собрания анализируются результаты, выявляются ошибки и

просчеты, составляется итоговый документ, который служит основой для подготовки следующего крупного мероприятия.

США: дефицит кадров в сфере информационной защиты

Бюро трудовой статистики США показало, что уровень безработицы в этом секторе составляет 3%, в то время как средний уровень по стране в два раза выше. Это хорошая новость для профессионалов информационной защиты и плохая – для бизнеса, пишет в журнале Chief Security Officer Тейлор Армединг (5 декабря 2013). Руководителям компаний сложно найти квалифицированного специалиста по информационным технологиям, еще труднее – профессионала, способного возглавить ИТ отдел.

Председатель организации Cybersecurity Credentials Collaborative Марк Нобл заявил в интервью BankInfoSecurity, что был вынужден на год задержать реализацию одной крупной программы, поскольку не мог заполнить вакансии по информационной защите. Такое положение он объясняет, в частности, быстрым изменением ландшафта рисков: «всегда требуется время, чтобы освоить новые технологии, регулярно предлагаемые рынком, изучить их уязвимости, приспособить к особенностям организации». Успешно работать с динамически меняющейся картиной рисков и угроз могут лишь те, кто способен быстро учиться и овладевать новыми знаниями, подчеркивает Нобл. По его мнению, криминал «всегда на 10 шагов впереди нас».

Глава службы информационной защиты – нечто большее, чем технически подготовленный специалист, отмечают эксперты. Он (она) в идеале должен разбираться в таких дисциплинах как маркетинг и финансы, правовые вопросы. В большинстве организаций на этой должности хотят видеть человека, который помимо своей специальности понимал бы бизнес компании, в целом отрасль экономики.

Другая проблема – не до конца понятное место, которое должен занимать руководитель информационной защиты в структуре компании. Кому он должен подчиняться – первому лицу, совету директоров, директору по безопасности или финансовому директору? На этот вопрос нет однозначного ответа. Но ясно, что нельзя стать эффективным руководителем, даже с прекрасной технической подготовкой, если не хватает знаний и навыков в таких областях как бизнес и право, если отсутствуют такие личностные качества как коммуникабельность, лидерские амбиции.

С другой стороны, топ-менеджмент ряда организаций недооценивает значение этой позиции, рассматривая ее как ничем не примечательную должность в среднем звене управления. Когда происходит утечка информации, есть на кого взвалить вину независимо от конкретной причины. Глава отдела ИТ рассматривается скорее как «мальчик для битья», нежели ценный креативный кадр, от работы которого не в последнюю очередь зависит успешная работа всей компании, ее конечные результаты.

Чтобы избежать ошибки в приглашении нужного специалиста, руководителям компании надо хорошо изучить слабые места, уязвимости в системе информационной защиты компании, обсудить их с кандидатом на вакантное место. А это уже

определенный риск, поскольку могут быть затронуты чувствительные аспекты, связанные с конфиденциальной информацией.

Эксперты прогнозируют, что дефицит кадров в этой специальности сохранится, как минимум, ближайшие пять лет, и предлагают решительно пересмотреть учебные программы, введя наряду с кибербезопасностью такие предметы как право и финансы, предусматривать в рамках учебы стажировку в компаниях.

The Safe Hiring Manual: The Complete Guide to Employment Screening Background Checks for Employers, Recruiters, and Job Seekers

The Safe Hiring Manual: The Complete Guide to Employment Screening Background Checks for Employers, Recruiters, and Job Seekers
By Lester S. Rosen. Facts on Demand Press,www.brbpublications.com; 734 pages; $24.95

Читатель найдет в этой книге массу информации относительно background checks (проверка биографии и данных в резюме при приеме на работу). Весь материал выстроен на конкретных, реальных фактах, в том числе и судебных исках, которые вынуждены в ряде случаев подавать компании на своих сотрудников (по причине небрежно проведенной в свое время проверки кандидатов на свободные вакансии). В книге также рассказывается о судебных исках компаний против рекрутинговых агентств, услугами которых они воспользовались для поиска и найма работников.

Автор издания, Лестер Розен, по образованию юрист, руководитель фирмы Employment Screening Resources, которая специализируется на проверках. Он создал своего рода руководство, практическое пособие по вопросам найма/ Читатель знакомится с крайне полезной информацией по всем аспектам процесса проверки и найма на работу. В частности, с подробным вопросником для соискателя вакансии (где, кстати, упоминаются и темы, которых следует избегать в ходе собеседований и проверок по правовым и этическим основаниям).

Довольно большое место в книге отводится социальным сетям как важному источнику персональной информации. Сбор персональных данных регулируется законодательством, и этот момент также подробно освещается.

Работники кадровых служб, специалисты по охране предприятия, консультанты и представители малого бизнеса – все они найдут книгу ценным информационным ресурсом.

Экономический кризис и кражи в

розничных сетях

Исследовательская компания Global Retail Theft Barometer выпустила в конце 2013 года отчет о глобальных тенденциях, связанных с преступностью в розничной торговле.

Согласно докладу, потери от мелкого магазинного воровства (шоплифтинг), злоупотреблений среди персонала, краж и грабежей, осуществляемых организованной преступностью, а также административной халатности и ротозейства в среднем составляют сегодня 1.4 процента розничных продаж, что превышает данные за предыдущий, 2012 год.

Главной причиной роста преступности эксперты называют кризисное состояние экономики, как следствие - высокую безработицу. «В стране (США) множество семей, чьи доходы за последние годы упали, и многие стремятся всеми способами сохранить прежний, более высокий уровень жизни», - говорит Дэн Рейнольдс, вице-президент по продажам корпорации Checkpoint (csoonline.com, November 12, 2013).

Обычно люди оплачивают самое необходимое для жизни, продолжает Рейнольдс. Объектом же краж служат, как правило, высоко стоимостные вещи. Наибольшей популярностью пользуются модные аксессуары, джинсы, обувь, дорогое дамское белье, продукция Apple, электронные игры, GPS гаджеты, мобильные девайсы.

Кроме того, ритейлеры отмечают рост числа воровских шаек, которые врываются в магазины и крадут в больших количествах бритвенные лезвия, детские молочные смеси, лекарства и предметы косметики. Все эти вещи затем перепродаются на черном рынке за 30% цены.

Страны с наивысшим уровнем потерь – Бразилия Мексика (1.6% от общего объема продаж). Следом за ними США (1.5%). В самом низу таблицы – Япония (1%). Исследование проводилось путем опроса (письменных и телефонных интервью) представителей 160 000 магазинов по всему миру.

Все респонденты единодушно заявляют, что пока нет технологий, которые бы на 100% защищали от воровства. Поэтому наибольший эффект дают сочетания разных приемов и методов защиты. Важную роль играет обучение персонала. Немалое значение имеет использование таких технологий как электронные радиометки (RFID - микрочип для маркировки товара и его радиочастотной идентификации) и видеонаблюдение.

В ряде стран, в частности, в Германии и Великобритании, отчетливо прослеживается взаимосвязь между высокими затратами на охрану и сравнительно низким уровнем краж.