Охрана предприятия

№5 (39), 2014

Оглавление

Книжное обозрение

Industrial Espionage: Developing a Counterespionage Program

Охрана небоскребов. Конфликт поколений

10 лет назад, в первые годы после трагедии 9/11, практически все, кто проживал или работал в высотках Нью-Йорка и других крупных городов США, проявляли неподдельный интерес ко всему, что касалось вопросов безопасности. Эксперты вспоминают, как учебные классы ломились от желающих пройти курс тренинга по безопасности.

Но все постепенно забывается. Спустя десятилетие интерес людей к этому вопросу неумолимо угасает. Марк Райт, директор службы безопасности корпорации Brookfield Properties в Хьюстоне, проводит параллель с вождением автомобиля: «Мы уже забыли, что послужило причиной аварии 12 лет назад, и, как и прежде, не включаем поворотник, перемещаясь на соседнюю полосу движения» (Security Magazine, July, 2014).

Не только память виновата. Другое поколение подросло. Сегодня в США каждый третий работающий - в возрасте менее 34 лет. Следующее поколение привносит новые взгляды, подходы, мнения. Молодые считают, что усиленный контроль над обществом с использованием современных технологий – «не есть хорошо». Им кажется, что камеры видеонаблюдения буквально преследуют их везде и всюду. Такую тенденцию среди молодежи специалисты по безопасности называют «тревожной».

Ранее вестибюль в небоскребах традиционно служил местом ожидания и встречи. Соответственно внутренний дизайн отличался лаконичностью, скромностью. Сегодня молодые сотрудники офисов, расположенных в высотках, превращают вестибюли в тусовочные места с обязательным Wi-Fi. Ветеранам охраны это, разумеется, не нравится. Но ничего не поделаешь, приходится приноравливаться к новым веяниям, примиряться с мыслью, что те, кого они охраняют, уже не привязаны намертво к своим офисным столам.

Что остается неизменным, то это «оценка рисков» (risk assessment). Уровни рисков различаются не только по регионам, но и внутри каждого региона, где есть высотки. Деловой центр в Нью-Йорке, например, отличается мощным насыщением ультрасовременной технологией безопасности, включая усовершенствованные программы контроля доступа с оптическими турникетами и электронные считыватели для допуска в лифты. В Лос-Анжелесе картина более разнообразна. Одни офисные высотки обеспечены технологией по высшему уровню, а в небоскребах по соседству нет даже электронных пропусков.

Что касается жилых высоток, то здесь решающее значение приобретает экономия средств. Но многое зависит от класса домостроения. Высотки в категории люкс

обладают пятью уровнями контроля за доступом: у входа; в главном вестибюле; в лифтах, на площадках каждого из этажей (где дежурят консьержки); собственно квартиры, обеспеченные видеонаблюдением.

Но, конечно, поддерживать все пять уровней безопасности – дело не дешевое и большинство владельцев небоскребов позволить себе такую роскошь не могут. Они вынуждены обходиться ограниченным набором технологий и охранных услуг. Поэтому в подавляющем большинстве случаев задействованы лишь два уровня – охрана входа и консьерж в центральном вестибюле.

Важнейшие профессиональные компетенции в современной информзащите

Окончание. Начало см. в выпуске журнала №38

Архитекторы и расследователи информационной защиты

Архитекторы безопасности определяют (и корректируют при необходимости) соответствие корпоративной стратегии, решений и практик меняющейся бизнес среде, новым возникающим рискам, которые в значительной степени обусловлены появлением мобильных девайсов, облачных исчислений, Больших Данных, других инноваций. Расследователи также играют возрастающую роль в деле своевременного обнаружения и блокирования попыток взлома корпоративной сети, умышленных и случайных утечек. Угрозы могут возникать неожиданно и с любой стороны, как внутри, так и извне компании. Для их минимизации и предотвращения требуются высокопрофессиональные компетенции, позволяющие организовать процесс поиска проблемного места, что зачастую сопоставимо с поиском иголки в стоге сена.

Обеспечение безопасности кассовых терминалов

Кассовые терминалы – «горячая точка» в информационной защите, полагает Тайлер Шилдс, главный аналитик компании Forrester Research Inc. Она появилась сравнительно недавно, поясняет эксперт, и обусловлена тенденцией переноса объектов хакерских атак со стационарных, офисных компьютеров на мобильные системы и кассовые терминалы. В последнее время все чаще фиксируются нарушения безопасности именно в этой зоне – зоне кассовых терминалов. Здесь, по мнению Шилдса, для обеспечения безопасности компьютеров и программ требуются специальные знания и навыки, которыми не всегда обладают специалисты, занимающиеся общими вопросами информационной защиты предприятия.

Эксперты-хакеры как испытатели систем на прочность

Идея найма профессиональных хакеров неоднозначна по ряду аспектов, в том числе и этическому, но общепризнано, что появление таких людей в структуре информационной защиты может быть чрезвычайно полезным делом. Если касаться новых трендов в сфере безопасности, то обращают на себя внимание две любопытные

тенденции. Первая – возрастающий спрос на т.н. «этических» хакеров, которых нанимают для того, чтобы они опробовали установленную в организации систему защиты информации на прочность, надежность. Вторая тенденция – растущий спрос на специалистов, способных быстро находить, где, в каком месте произошел взлом или хакерская атака, или утечка данных, какие важные корпоративные данные скомпрометированы.

Специалисты с тренерскими навыками

Речь идет о специалистах, которые помимо своих основных профессиональных компетенций обладают способностями обучать персонал компании элементарным основам информационной защиты, давать доступные разъяснения относительно рисков и уязвимостей. Другими словами, учить людей тому, чему те сами никогда не научатся. Такой подход объясняется двумя причинами. Во-первых, тем, что атаки все больше приобретают характер целевых, т.е. направленных на работников, обладающих доступом в корпоративные сети, хранилища данных. Такие покушения совершаются как через электронную почту, так и по телефонной связи, и через социальные медиа. Во-вторых, надо признать, что традиционные способы борьбы за безопасность, такие как ежегодные собрания или плакаты, призывающие соблюдать осторожность и бдительность, малоэффективны. С использованием смартфонов и облачных исчислений возникла особая необходимость в кропотливой работе с персоналом, в обучении людей строгим правилам безопасности.

Технологии эффективности видео аналитики

К. Мейер, автор статьи в августовском номере журнала Security Magazine (2014), обращает внимание, что человеческие возможности отслеживать ситуацию с помощью монитора видеонаблюдения весьма ограничены по времени: «наши глаза не предназначены для тщательного наблюдения, обнаружения тех или иных изменений в течение продолжительного времени. Уже через двадцать минут непрерывной работы у экрана монитора внимание начинает ослабевать».

Глава контрактной компании в военной сфере JL White & Associates Джеймс Уайт участвовал в установке и эксплуатации на одной из военных американских баз в Афганистане системы видеонаблюдения, которая обеспечивала 85%-ный уровень обнаружения (detection rate) и всего 2%-ную норму ложных сигналов. В программу видеоаналитики были введены такие параметры как размер объекта, его формы и текстура. «Если не задать системе точные параметры того, что вы хотите, то она будет реагировать абсолютно на любые изменения. Вопрос заключается в отсеивании ненужной информации, минимизации ложных сигналов. Если круглосуточное видеонаблюдение ограничивается тремя ложными сигналами в день, то, значит, она работает отлично», считает Уайт.

Эффективность видеоаналитики критически важна в системе СКУД, когда видеонаблюдение помогает охранникам обнаруживать нестандартное поведение, чреватое негативными последствиями, в частности, попытки несанкционированного проникновения в здание. В этом случае оно посылает тревожный сигнал дежурному

центра мониторинга, который анализирует ситуацию, оценивает риск, предпринимает адекватные меры.

Cezary Jozwiek – главный офицер по безопасности польской компании Naftoport рассказывает о системе видеонаблюдения, установленной в морском порту. Она включает:

- видеонаблюдение с аналоговыми, инфракрасными и цифровыми камерами;

- видеоаналитику;

- тревожную сигнализацию, предназначенную для предотвращения несанкционированных вторжений;

- систему охраны периметра, которая состоит из сонара, радара, СКУД, системы автоматической идентификации судов, системы спутникового мониторинга GPS.

Все вышеперечисленные технологии интегрированы на единой платформе PSIM, что позволяет оператору работать с одним интерфейсом вместо нескольких одновременно. Когда случается инцидент, оператор, он же дежурный диспетчер службы безопасности, получив сигнал, принимает ответные меры. Служба безопасности имеет в своем распоряжении пеший, морской и авто патрули. Для отдельных случаев предусмотрено взаимодействие с полицией, погранслужбой, пожарной командой.

Интеграция видеоаналитики с другими технологиями, не связанными с видеонаблюдением, считает Уайт, открывает массу новых возможностей. К примеру, если охранный периметр снабжен сейсмическими сенсорами, которые посылают тревожный сигнал, оператор, имея в своем распоряжении единый интерфейс, может тут же отследить через камеры видеонаблюдения тот участок периметра, откуда сигнал поступил, не теряя времени на переключение с одной системы на другую.

Эксперты полагают, что использование интеграционных схем выгодно не только технологически, но и с финансовой точки зрения, поскольку умные компьютеры заменяют людей.

Эффективные технологии видеонаблюдения на стадионах

Строительство MetLife Stadium в штате Нью-Джерси (США), домашнего стадиона для двух футбольных клубов, New Your Football Giants и New York Jets, обошлось этим клубам в сумму 1.6 миллиардов долларов. Его открытие состоялось в апреле 2010 года. Вместимостью 82 500 зрителей, это один из крупнейших футбольных стадионов в США.

Не так давно администрация стадиона заменила PTZ камеры слежения (PTZ - сокращение от Pan, Tilt, Zoom, что обозначает возможности камеры вращаться в двух плоскостях и приближать изображение) на новые панорамные камеры с диапазоном

180 градусов.

Футбольные состязания, концерты и другие мероприятия, привлекающие десятки тысяч людей, требуют немалых усилий администрации, прежде всего службы охраны, чтобы отслеживать поведение футбольных фанатов, управлять огромными массами, обеспечивать своевременное вмешательство, включая оказание медицинской помощи. Поэтому главной целью обновления системы видеонаблюдения администрация формулирует «обеспечение здоровья и жизни людей, предотвращение конфликтов, создание и поддержание среды безопасности» (Security Magazine, July, 2014) .

Одна из главных забот службы безопасности – расследование инцидентов, которое, как правило, сталкивается с различными трактовками и версиями со стороны участников конфликта и независимых свидетелей. Зачастую решающую роль в нахождении истины играют видеозаписи.

Прежние (PTZ) камеры слежения, установленные внутри чаши стадиона, фиксировали ситуацию в том или ином секторе только по команде диспетчера, когда инцидент уже был в разгаре или в фазе своего завершения. С установкой новых камер обеспечен мониторинг каждого из 82 500 мест постоянно и в режиме реального времени. Архивация данных позволяет офицерам собственной службы безопасности, равно как и представителям правоохранительных органов, прокручивать назад последовательность событий и воссоздавать достоверную картину произошедшего.

Среди других задач, которые выполняет видеонаблюдение – фиксация забытых на стадионе вещей, мониторинг сканирования безопасности на входах в стадион, расследование несчастных случаев, контроль работы персонала, осуществление антитеррористических мероприятий.

На замену старому оборудованию пришли 130 Arecon Vision мегапиксельные камеры, включая компактные 10-мегапиксельные, установленные по всей чаше стадиона и позволяющие держать под визуальным контролем каждое зрительское место во всех секторах. Панорамные 8PM камеры с амплитудой разворота в 180 градусов установлены вокруг стадиона, они помогают контролировать подходы к стадиону. 3MP камеры с технологией WDR («расширенный динамический диапазон») оборудованы при входе на территорию стадиона, там, где охранниками проводится первичная проверка, досмотр посетителей.

Мониторинг и управление видеонаблюдением осуществляется с центрального пункта службы безопасности. В планах администрации стадиона - включать полностью систему видеонаблюдения минимум за сутки до дня мероприятия, фиксируя и записывая все, что происходит на стадионе и вокруг него.

Hilton предлагает гостиничный ключ на персональном смартфоне

Как сообщает журнал Security Magazine, всемирно известная гостиничная корпорация Hilton планирует разрешить своим постояльцам использовать личные смартфоны для регистрации, выбора номеров и даже в качестве ключей.

До конца этого года корпорация запустит проект по использованию цифровых технологий в 4 000 отелях более чем 80 стран. По заявлению топ-менеджера корпорации Джеральдин Кэлпин, «такое решение принято на основе тщательного анализа предпочтений 40 миллионов клиентов, проведенных опросов, изучения постов социальных сетей, других информационных ресурсов. В результате выяснилось, что гости желают большей свободы выбора».

Кэлпин сослалась на организованное корпорацией исследование, которое показало, что 84% разъезжающих по миру бизнесменов предпочитают сами выбирать для себя гостиничный номер. Hilton готов предоставить клиентам возможность самим выбирать комнату, номер комнаты, категорию (в зависимости от наличия) при помощи персонального мобильного девайса.

Надо отметить, что первое, пилотное, приложение, получившее название Conrad Concierge, было выпущено и опробовано еще в 2012 году. Его итоги обсуждались этим летом, тогда же было принято решение перейти к долгосрочной программе внедрения информационных технологий в практику обслуживания клиентов.

Тем, кто пользуется услугами Hilton, начиная со следующего года, будут предлагать использовать персональный смартфон в качестве гостиничного ключа. Предполагается, что такая услуга охватит в 2015 году все отели сети в США, а к концу 2015 года – большинство гостиниц Hilton в мире.

Президент Hilton International Кристофер Нассетта подчеркивает, что поскольку путешественники охотно пользуются своими смартфонами в качестве посадочного талона в гражданской авиации, то, скорее всего, не откажутся и от функции гостиничного ключа.

«Мы потратили несколько последних лет, чтобы опробовать и проверить разные варианты реализации этой идеи, и в результате сумели создать технологию электронного ключа на смартфоне, которая одновременно безопасна, легко доступна для пользователя и экономически выгодна для корпорации», отметил Нассетта в специальном заявлении.

«Открытый» офис – головная боль для службы безопасности

Сегодня все больше фирм предпочитают выбирать для себя т.н. «открытый» офис (open floor plan - пространство этажа, ограниченное мебелью, подвижными перегородками или другими способами, но не стенами здания, когда весь или значительная часть персонала располагается в одном большом помещении). В таком планировании есть свои преимущества, заключающиеся, прежде всего, в создании условий для более тесного и дружного взаимодействия между сотрудниками организации. Но для офицеров по безопасности «открытый» офис представляет немалую головную боль, отмечает Лари Понемон в статье, размещенной в онлайновом журнале Chief Security Officer (August, 25, 2014). Охранникам приходится решать сложные проблемы, связанные с защитой имущества, интеллектуальной собственности, корпоративных данных. В чем эти проблемы и как их решать?

Опасность визуальной кражи (visual hacking)

Речь идет о том, что гости, клиенты, партнеры, получающие доступ в заполненное рабочими столами пространство, а также «собственные» злоумышленники имеют все шансы подсмотреть конфиденциальную информацию с включенных экранов компьютеров, с открытых документов, незаметно отснять содержание с помощью смартфонов, не говоря уже о специализированной шпионской аппаратуре. Эксперты советуют использовать специальную защитную технологию, в частности, электронный «экран» 3M ePrivacy Filter, который идентифицирует пользователя с помощью веб-камеры и снижает угол обзора, а также инструктировать персонал, чтобы не оставляли компьютеры включенными и документы на столе, уходя на обед или совещание, обучать другим мерам предосторожности.

Опасность подслушивания

Чтобы минимизировать риски подслушивания служебных разговоров, специалисты рекомендуют применять специальные технологии преобразования звуков (white noise, pink noise), выделить отдельное (закрытое) помещение для телефонных служебных разговоров и рабочих совещаний, шире использовать обмен сообщениями и файлами по внутренней компьютерной сети.

Риск обычных краж

По некоторым исследованиям, в общем объеме утраченных ноутбуков офисные кражи занимают 12%. Вот что советуют эксперты по безопасности:

- приучать персонал к тому, чтобы не оставляли без присмотра свои портфели, папки с документами, любые носители информации;

- оборудовать специальные ящики с замками для хранения служебных документов;

- предусмотреть для компьютеров надежные кодовые замки с металлическим кабелем;

- Все девайсы и носители конфиденциальной информации снабдить шифровальными ключами и программой удаленного стирания компьютерных файлов;

- установить камеры слежения, чтобы а) дисциплинировать персонал; б) облегчить расследование краж и прочих инцидентов безопасности.

Как обеспечить защиту от сторонних лиц и организаций

В современном взаимосвязанном мире бизнес не может нормально функционировать без множества нитей, связывающих его с поставщиками, подрядчиками, аффилированными структурами, партнерами и прочими третьими организациями и личностями. В то время как эксперты продолжают называть «безответственного инсайдера» наиболее уязвимым звеном в системе охраны предприятия, внешний партнер с точки зрения рисков и угроз достоин такого же, если не большего, внимания

службы безопасности.

Р. Райзер и С. Ганов, адвокаты компании Faruki Ireland & Cox., авторы Белой книги под названием “Traitors in Our Midst: The risk of employee, contractors and third parties in the age of the Internet of Things and why security in depth remains critical to risk management.”, отмечают, что «межсетевые экраны, системы кодов и паролей по-прежнему играют важную роль, но не обеспечивают полную защиту бизнеса» (csoonline, June 30, 2014).
Относительно недавний пример: взлом баз данных крупного ритейлера Target. Хакеры осуществили фишинговую атаку с использованием электронной почты партнера Target – компании, занимающейся установкой систем отопления и кондиционирования. Один из сотрудников этой компании легкомысленно щелкнул на вредоносную ссылку и, в конечном счете, скомпрометированными оказались миллионы кредитных карт, принадлежащих клиентам Target.

Хакерские взломы через сторонние организации становятся все более распространенными, считает Поль Трюлав, вице-президент SailPoint. Даже такой гигант рынка как корпорация AT&T подверглась мощной атаке через одного из провайдеров, в результате чего хакеры овладели персональной информацией клиентов AT&T, обладателей мобильных девайсов, в том числе данными о датах рождения и номерах страховок.

Причина подобных провалов, по мнению экспертов, заключается в том, что при заключении партнерских и подрядных договоров не уделяется должного внимания вопросам обеспечения безопасности бизнеса со стороны контрактора. Другая причина – наем временных работников, зачастую без участия службы безопасности и управления кадров. Плюс ко всему такие работники нередко остаются вне контроля СКУД и других систем безопасности, отслеживающих доступ и перемещения постоянного (штатного) персонала. Работники по контракту обычно приносят на временную работу собственные компьютеры и программы, которые не проходят очистку и контроль в корпоративной сети. Прибегая к аутсорсингу, популярность которого из года в год растет, компании интересуются, главным образом, стоимостью услуг, а не уровнем безопасности.

Чтобы минимизировать риски, эксперты советуют не забывать о базовых мерах защиты предприятия. Например, менять пароли всякий раз при приобретении (в том числе через партнеров) новых девайсов, использовать мульти-факторную идентификацию.

Кроме того, во время подготовки контракта с третьей стороной необходимо предусматривать такие компоненты как:

- информационная защита;

- охрана прав личности (в т.ч. персональных данных);

- анализ рисков и угроз;

- обязательство следовать правилам и инструкциям по безопасности;

- согласие на проведение внутренних аудитов и расследований;

- меры борьбы с коррупцией.

Особенно важно в этом перечне заручиться согласием партнера на проведение аудитов безопасности и такие аудиты практиковать.

Составные части эффективной программы управления рисками на предприятии

Эксперты и постоянные авторы онлайнового журнала Security Magazine Дж. Бреннан и Л. Мэттис опубликовали в июльском выпуске статью, где рассказывают о результатах многомесячного изучения элементов претендующей на эффективность программы обнаружения, анализа и управления рисками на любом предприятии, независимо от того, в локальном или глобальном масштабе предприятие функционирует. Они отмечают, что каждый, даже малозаметный риск, может обернуться существенными потерями для предприятия, не только финансовыми, но и репутационными. Поэтому критически важно сформировать такую программу, которая бы охватила все потенциальные риски и угрозы.

Первым шагом на этом пути эксперты называют документированное создание портфеля всех возможных рисков, с которыми сталкивается или может столкнуться компания. Это возможно благодаря проведению разведки и тщательного анализа всех без исключения сторон и аспектов деятельности компании на предмет обнаружения подстерегающих организацию опасностей.

В процессе осуществления данной программы собирается, систематизируется, обрабатывается и анализируется информация применительно ко всем функциям организации. В конечном итоге полученные данные ложатся в основу стратегического планирования. Разумеется, такие данные должны быть абсолютно адекватными реальности, пользоваться доверием со стороны принимающих решения менеджеров.

Как только матрица рисков заполнена, необходимо выделить приоритетные угрозы, т.е. такие, какие несут наибольшую опасность для жизнеспособности и устойчивости предприятия. После этого можно приступать к проработке решений по минимизации рисков для разных функций и направлений деятельности организации. Одни риски требуют использования сложных и дорогостоящих методологий. Другие можно предупредить, не затрачивая больших сил и средств, например, через инструменты страхования. Наконец, некоторые риски можно вообще не принимать во внимание, если они потенциально незначительны, а борьба с ними требует несоразмерные ущербу значительные ресурсы.

Следующий шаг – формирование правил, процедур и процессов управления рисками по всему предприятию, конечная цель которых – научить весь персонал адекватно действовать в самых разных сложных, кризисных ситуациях, сохраняя устойчивость организации. Разумеется, предполагается, что работники тренированы, осознают свою роль, функцию, ответственность.

Эффективность и функциональность корпоративных политик и процедур подтверждается с помощью аудитов, проверок, инспекций, объективных оценок. Если

случается прокол или обнаруживается уязвимость, вносятся коррективы, предотвращающие повторение. Также все инструкции подвергаются изменениям, когда те или иные риски исчезают или, напротив, возникают новые угрозы.

Мобильные технологии и безопасность в сфере здравоохранения

В канадском онлайновом издании Canadian Security Magazine за 25 августа сего года размещена статья Дж. Холлерана, посвященная вопросам безопасности мобильных технологий в сфере здравоохранения.

Мобильные технологии получают мощное развитие во всех сферах бизнеса и общественной жизни, но особенно активно захватывают здравоохранение. Благодаря возможностям быстро получать данные и незамедлительно реагировать (когда часто несколько секунд решают вопрос о жизни и смерти) здравоохранение превращается в глобально взаимосвязанную высокотехнологичную систему. Сегодня медицинские учреждения по степени насыщенности мобильными носителями информации, специализированными мобильными приложениями находятся в числе мировых лидеров.

Соответственно возрастают и риски. По данным исследователей Ponemon Institute, 90% медицинских организаций в Северной Америке, так или иначе, подвергались информационным утечкам на протяжении последних двух лет. Подавляющее большинство согласились на использование в служебных целях BYOD (принеси в офис свой девайс – «мобильный офис»), хотя более половины из них не уверены, что данная практика гарантирует безопасность.

Автор публикации анализирует 5 принципов безопасности, которым следует, по его мнению, следовать при использовании мобильных носителей в лечебных учреждениях.

1. Обеспечить безопасность BYOD

Начинать надо с конечного пользователя. Работники медучреждений применяют собственные девайсы в разных целях, в частности, для хранения служебных баз данных. Они также входят в офисную почту и переписку, пользуются внутренним веб-сайтом (интранетом), работают со служебными документами. Автор рекомендует принять на вооружение программное решение по управлению мобильными устройствами (enterprise mobility management – EMM), обеспечивающее административный контроль над приложениями, с которыми работают служащие (например, допуск к корпоративным данным, разрешение на хранение информации на мобильных устройствах).

2. Шифрование данных

Шифры играют ключевую роль в защите информации. Автор рекомендует использовать программный продукт для шифрования наряду с межсетевыми экранами и прочими распространенными средствами информационной защиты.

3. Обеспечить защиту от вирусов

Организации здравоохранения, использующие мобильные устройства с открытыми платформами, особенно подвержены риску заражения зловредными вирусами. Последние широко применяются преступниками для взлома файлов с персональными данными и корпоративной информацией. Чтобы минимизировать риски, необходимо предусмотреть надежную защиту на всех уровнях информационной инфраструктуры – собственно компьютеров, их программ и корпоративных сетей.

4. Строжайший контроль за использованием мобильного офиса

Хорошо организованная система компьютерного контроля позволяет администратору информационных технологий следить за трафиком данных и принимать немедленные меры в случае нарушения пользователями BYOD предписаний и инструкций по безопасности.

5. Предусмотреть возможности дистанционного стирания данных

Поскольку медицинским работниками часто приходится работать вне своих учреждений (выезды к больным и другие служебные причины), необходимо предусмотреть возможность уничтожения служебной информации на мобильных носителях в случае потери или кражи. Сегодня на рынке имеются в наличии специальные приложения, благодаря которым можно стирать служебные данные без ущерба для персональной информации владельца мобильного устройства.

Охрана паркингов

По данным американских экспертов, до 40% преступлений совершаются в паркингах. Официальная статистика США гласит: в период 2004 - 2008 гг. ежегодно фиксировалось более 100 000 покушений на собственность в коммерческих автопаркингах и гаражах. С 1999 года по начало 2014 только на территории паркингов, принадлежащих религиозным организациям, было совершено 792 преступления с летальным исходом.

Пол Гера возглавляет службу безопасности церковного округа в городе Woodland (в окрестностях Хьюстона). Церкви округа посещает множество прихожан – до 18 000 по воскресениям, до 50 000 по большим религиозным праздникам. «Наша задача, - говорит Гера, - не столько отвечать на инциденты, сколько стараться их предотвращать» (Security Magazine, August, 2014).

Освещение – одно из наиболее эффективных средств борьбы с преступностью в паркингах. Мощные светильники обеспечивают мониторинг территории в деталях с помощью камер видеонаблюдения. Светодиодные лампы автоматически включаются, реагируя на движение автомобиля или человека. Одномоментно сигнал поступает к диспетчеру, который следит за происходящим на экране монитора и может вступить в разговор с незнакомым лицом благодаря специальным устройствам, вмонтированным в систему видеонаблюдения.

Директор по развитию компании ATC International (штат Флорида) Маркус Иорено

отмечает, что постоянно совершенствуемые технологии повышают эффективность охраны. К примеру, в многоэтажном коммерческом паркинге в Майами Бич установлены переговорные устройства Talkaphone и система видеонаблюдения Video Insight HD, интегрированные на единой программной платформе. Использовать систему PA (громкоговорящая система оповещения), дистанционно управляемую одним диспетчером намного выгоднее и эффективнее, чем держать патрульную службу. Офицер безопасности может обнаружить в паркинге незнакомца, бродящего по этажам и рассматривающего автомобили. Возможно, он просто забыл, где припарковал свой лимузин. Но, не исключено, у него другая цель. В любом случае дежурный офицер по безопасности может, не выходя из диспетчерской комнаты, обратиться к нему по системе PA, выяснить причину блужданий, если необходимо, помочь и подсказать, куда надо обратиться, чтобы решить проблему.

Применение интернет технологий позволяет экономить кучу денег. Если бы ранее, каких-нибудь 10-15 лет назад, пользователь хотел связать видеонаблюдение, освещение, переговорное устройство на базе одной мониторинговой платформы, то ему пришлось бы тянуть километры кабелей, что обошлось бы в хорошую копеечку. Программные решения IP не только облегчают интеграцию разных видов и средств охраны, но намного удешевляют ее.

Маркус Морено также обращает внимание на необходимость заблаговременно планировать установку новых технологических систем охраны. В идеале необходимо рассчитывать структуру безопасности перед строительством, на этапе проектирования паркинга. Так можно сэкономить до 40% средств, необходимых на установку охранных систем. Но если стоит задача переоснащения уже действующих паркингов, то Морено советует внимательно изучить имеющуюся инфраструктуру, особенно доступ к электросети, что также может сократить смету перестройки.

Помимо противодействия криминалу, средства охраны паркингов играют важную роль в расследовании несчастных случаев и автомобильных аварий.

Охрана предприятия с помощью бэкграундных фильтров

Окончание. Начало см. в выпуске № 38

Многие организации пренебрегают регулярным аудитом программ бэкграундной проверки, который бы устанавливал соответствие корпоративных предписаний и процессов изменениям в бизнес среде и в сфере регуляции. Эксперты советуют разрабатывать и иметь всегда в наличии письменную инструкцию, которая бы документировала, кто (кандидат на какую должность) должен подвергаться обязательной проверке, что именно необходимо проверять, как полученная в результате проверки информация влияет на принятие окончательного решения о приеме на работу. Такой документ гарантировал бы соблюдение организацией принятых в ней правил проверки, минимизировал бы кадровые ошибки.

Эксперты советуют начинать проверку криминальной истории с данных по месту постоянного проживания, учебы, предыдущей работы. Кроме того, было бы полезно также заглянуть в федеральные архивы, так как соискатель мог «проколоться» во

время поездок, путешествий. Это тем более необходимо, если есть подозрения, что кандидат на работу скрывает свое пребывание (временное проживание) в тех или иных местах.

В последнее время становится обязательным правило перепроверять предоставляемые соискателем данные о времени и месте прежней работы, о зарплате и занимаемой должности, связываясь непосредственно с его/ее бывшим работодателем. Правда, не всегда удается контактировать со всеми работодателями, так как какие-то фирмы закрываются, люди уходят из бизнеса…. В таких случаях целесообразно попросить соискателя представить хоть какие-нибудь документы, подтверждающие указанные им данные о работе и зарплате.

Точно также эксперты рекомендуют обращаться в учебные заведения, указанные в резюме. Нередки факты прямого обмана, основанные на уверенности, что никому не придет в голову проверять представленную информацию. Особенно важно удостовериться, что прилагаемые к резюме дипломы не являются «липой», сфабрикованной мошенниками, которых множество развелось на данной стезе не только в России, но и в Америке.

Рекомендуется также не игнорировать и данные дорожной полиции, тем более, если предлагаемая должность предполагает разъезды за рулем на собственном или офисном автомобиле. Здесь важно обратить внимание на характер возможных нарушений. Езда в алкогольном состоянии или под воздействием наркотиков – серьезная причина отказать в приеме на работу.

Когда конкуренция на рынке, в том числе и за таланты, возрастает, времени на проведение тщательных проверок критически не хватает. Затянув время на принятие решения, можно выпустить из рук хорошего специалиста, в котором нуждается организация. Это риск. Но не менее рискованно брать на работу кого попало, ограничиваясь проверкой исключительно профессиональных компетенций. В таких случаях выбор всегда за организацией.

О чем надо помнить, разрабатывая стратегию борьбы с инсайдерством

Любой бизнес, независимо от его размеров и отраслевой специализации, сталкивается с серьезной угрозой в лице инсайдерской деятельности. В одном из последних исследований Ponemon Institute отмечается, что этой проблемой озабочены 88% организаций. В то же время, как показал опрос, большинство не имеют ясного представления о том, как бороться с этой опасностью.

Топ менеджеры компании Accuvant, занимающейся консалтингом и исследованиями по корпоративной безопасности, Дж. Кларк и Дж. Робинсон подчеркивают необходимость иметь в любой организации строгую стратегию борьбы с инсайдерством, которая в обязательном порядке включала бы технологии, процессы, меры контроля. Авторы статьи в журнале Chief Security Officer выделяют пять вопросов, которые важно иметь в виду при разработке и осуществлении такой стратегии.

1. Сбалансированное финансирование

Формулируя программы корпоративной безопасности, компании зачастую не имеют навыков и методологии сопоставлять внутренние риски с бюджетным балансом. По некоторым исследованиям, почти половина организаций не вкладывают средства в технологии, призванные минимизировать риски, исходящие от инсайдеров. Затраты на эти технологии не сопоставляются с потенциальными потерями. Между тем, согласно исследователям, более половины электронных преступлений, так или иначе, связаны с инсайдерами.

2. Не закрывать глаза на внутренние угрозы

Многие организации не рассматривают инсайдерство главным приоритетом в стратегии безопасности, т.к. зачастую активность инсайдеров остается незамеченной, во всяком случае, продолжительное время. А когда обнаруживается, то подавляющее большинство компаний предпочитают не предавать факты огласке, дабы не повредить репутации. Отчасти подобное отношение обусловлено самоуспокоением, что, мол, «такое у нас никогда не случится».

3. Это в первую очередь проблема человеческого фактора

Слишком часто руководители организаций сводят инсайдерство к проблеме киберзащиты и технической стороне дела. Это в корне неверный подход, т.к. решающую роль играет человеческий фактор, желание и умение управленцев уделять большое внимание обучению персонала, разъяснять, насколько важно соблюдать правила защиты информации для каждого и компании в целом. Но одного обучения мало. Оно должно дополняться регулярной инвентаризацией имущества, состоянием паролей, шифров, соблюдением соответствующих политик и инструкций.

4. Поддерживать высокий уровень технологической защиты

На рынке появляются новые технологии, помогающие в борьбе с инсайдерами. Это, в частности, продвинутые аналитические решения, отслеживающие поведение работников организации, реагирующие на отклонения от нормы. Другие технологии помогают в обучении людей мерам безопасности.

5. Баланс между контролем и доверием

Некоторые руководители не хотят использовать технологии поведенческого мониторинга из-за боязни прослыть «плохими парнями», вызвать неприязнь и недоверие в коллективе. Что здесь можно посоветовать? Скажем, взять на вооружение технологии, функционирующие неназойливо, ненавязчиво, деликатно. Но, с другой стороны, нельзя забывать о возможных нарушениях закона о privacy. Выход в том, чтобы ничего не скрывать от сотрудников, проводить политику контроля за ситуацией с полного согласия и при понимании со стороны коллектива.

Охрана предприятия в США: тенденции и прогнозы до 2017 г.

Корпоративные службы безопасности в США пережили нелегкое время кризиса 2007-

2009 гг., когда их бюджеты нещадно сокращались. Но, начиная с 2011 г., в Америке наблюдается устойчивый рост расходов бизнеса как на операционные функции служб безопасности (физическая охрана, внутренние расследования, противодействие мошенничеству, разведка и т.п.), так и на защиту информационных технологий.

Международная организация ASIS International провела исследование основных тенденций в американской индустрии безопасности и перспектив ее развития в 2014 – 2017 гг. Некоторые данные и цифры из отчета опубликованы в августовском номере онлайнового журнала Security Management.

За последние два года расходы на охранные продукты и услуги в США возросли на 20%, до 341 миллиардов долларов в 2014г. Расчеты предсказывают 10% рост в 2015 году. Причем львиная доля прироста приходится не на крупные корпорации, а на малые и средние предприятия. Темпы увеличения инвестиций в информационную защиту несколько опережают соответствующие темпы роста вложений в операционные функции.

Покупательский бум охватывает в первую очередь такие продукты и услуги как видеонаблюдение, СКУД, защитные интернет программы и решения, консалтинг безопасности, проверка и тренинг персонала, эксплуатация и поддержка технологий безопасности.

Примерно, каждая третья американская организация планирует увеличивать, в среднем на 12% в год, расходы на проверку персонала (employee screening). Это, прежде всего, касается ритейлеров, компаний, занимающихся профессиональными и техническими услугами, главным образом, малого бизнеса. Прогнозируется, что компании среднего размера будут наращивать расходы на контроль периметра и системы СКУД. Информационные, транспортные и образовательные организации продемонстрируют впечатляющий рост расходов (каждая третья организация до 20%) на видеонаблюдение.

По данным ASIS, сегодня в США насчитывается 2.7 миллионов занятых полное рабочее время в частной охране. Здесь не учтены те, кто работает в индустрии безопасности, но не связаны напрямую с охранной деятельностью (бухгалтерия, маркетинг, т.п.). Примерно один миллион из этой цифры – специалисты по информационным технологиям, дисциплине, которая была малоизвестна до 1990 года.

Настоящий кадровый бум происходит в сегменте информационной защиты. Число только аналитиков здесь возрастет к 2022 г. почти на 40%, что означает появление новых 100 000 рабочих мест. Они сегодня могут рассчитывать на компенсации в размере $80 000 в год для рядовых, $92 000 для старших аналитиков.

Что касается оперативной сферы безопасности, то здесь рост охватывает продукты и услуги, но не кадровое прибавление. Количество вакансий будет увеличиваться, но незначительно, что, возможно, объясняется внедрением эффективных технологий. Более половины из 1.7 миллионов оперативников (57%) работают охранниками, 17% - функциональные специалисты, 11% - управленцы, 9% - администраторы, 5% - функциональные менеджеры.

Спрос и зарплаты в американской охранной индустрии

Столь высокий спрос на талантливых специалистов в сфере корпоративной безопасности, как сегодня, никогда ранее не отмечался в США, пишет на сайте csoonline.com (September 9, 2014) Дж. Халм. По данным исследовательской организации Gartner, в этом году затраты на охрану предприятия, включая зарплаты охранников и офицеров безопасности, в США возрастут минимум на 8%. Между тем, со всех сторон слышатся жалобы, что специалисты в этой сфере не получают того, что на деле заслуживают.

Опрос, проведенный изданием Chief Security Officer среди руководящего состава служб корпоративной безопасности, показал, что в текущем, 2014 году средняя годовая зарплата топ менеджеров - $179 600, что ниже прошлогоднего показателя - $180 100. Происходит любопытная вещь – компании жалуются на трудности с привлечением талантов, с удержанием у себя хороших специалистов по безопасности, уверяют, что делают всё, чтобы привлечь и закрепить таланты, всё, кроме…повышения жалования.

Еще немного американской статистики. Среди 6 крупнейших мегаполисов США наиболее высоко оплачиваемые руководители СБ работают в Нью-Йорке и Сан Франциско (зарплаты в диапазоне $150 000 - $218 000). В Бостоне и Вашингтоне они зарабатывают $140 000 – $205 000. В Денвере и Чикаго $109 000 – $200 000. Однако, если принять во внимание разницу в стоимости жизни в разных городах (еда, лечение, жилье, транспорт), то получается, что реальные доходы выше в Денвере и Чикаго, где жить намного (на 48%) дешевле, чем в Нью-Йорке или Вашингтоне.

Наибольший дефицит американский рынок труда в сегменте охраны предприятия испытывает в специалистах по защите информации и информационных технологий. Одна из главных причин дисбаланса, полагают эксперты, – нежелание компаний платить таким специалистам высокие зарплаты. Подобный подход зачастую объясняется элементарной недооценкой значения информационной защиты. Говорит Джеймс МакМёрри, основатель и глава компании Milton Security Group: «Мы видим, что рынок постепенно осознает важность безопасности для бизнеса, но еще недостаточно, чтобы вкладывать в безопасность адекватные средства. Во многих случаях бизнесмены просто не представляют себе, насколько трудоемкой, сложной является работа по информзащите».

Другая причина проблемы - неумение увязывать результаты информационной защиты с конечными финансовыми итогами бизнеса (bottom line). Брайан Мартин, президент консалтинговой компании Digital Trust LLC: «Компания заключает в себе: социальный организм (social entity), клиентов и акционеров. Все три категории заинтересованы в том, чтобы избегать инцидентов безопасности, и, казалось бы, понимают необходимость инвестировать в специалистов высокой квалификации. С другой стороны, компаниями движут, прежде всего, мотивы прибыли, бонусов, сокращения себестоимости, снижения затрат. Эти две тенденции накладываются и конфликтуют между собой».

В результате во многих организациях сложилась ситуация, при которой качественно управлять рисками сложно, зато легко подвергнуться критике при малейшем сбое –

ведь никто из топ менеджмента не хочет брать на себя ответственность за нанесенный утечками и кражами данных материальный и репутационный ущерб. Б. Мартин подчеркивает, что, конечно, при неудачах проще простого уволить ответственного за информационную безопасность. Но проблему такими мерами не решить до тех пор, пока весь менеджмент, включая первых лиц, не почувствует свою персональную ответственность за обеспечение надежной безопасности предприятия.

Industrial Espionage: Developing a Counterespionage Program

Industrial Espionage: Developing a Counterespionage Program
By Daniel J. Benny; Reviewed By Paul D. Barnard, CPP
CRC Press; crcpress.com; 214 pages; $69.95.

Книга предназначена для тех, кто хочет выстроить эффективную систему противодействия промышленному шпионажу. По мнению автора, большинство монографий по этой тематике не достигают этой цели. Чтобы помочь читателю практически осуществить программу борьбы с промышленным шпионажем, автор книги провел глубокий и всесторонний анализ конкретных, реальных фактов, и пришел к убеждению, что вполне реально защитить интеллектуальную собственность, бизнес секреты с помощью эффективной программы.

Читателю разъясняется разница между промышленным шпионажем и конкурентной разведкой, подробно рассматриваются такие темы и вопросы как разведывательный цикл, способы сбора развединформации, традиционные методы разведки и киберугрозы, меры предосторожности и защиты во время деловых поездок и путешествий, тренинг по повышению информированности и осведомленности о рисках и опасностях промышленного шпионажа, фундаментальные основы физической и информационной защиты.

Отдельный раздел посвящен вопросам создания и функционирования корпоративной службы безопасности. Заключительная часть книги представляет список организаций и агентств в качестве ресурсов контр-шпионской деятельности, включая контактную информацию.